SOPHOS

SafeGuard PortProtector 3.30 SP6

User help

Document date: March 2010

Important Notice

This guide is delivered subject to the following conditions and restrictions:

- This guide contains proprietary information belonging to Sophos. Such information is supplied solely for the purpose of assisting explicitly and properly authorized Sophos SafeGuard PortProtector users.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic or mechanical, without the express prior written permission of Sophos.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this guide is furnished under a license. The software may be used or copied only in accordance with the terms of that agreement.
- Information in this guide is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- The information in this document is provided in good faith but without any representation or warranty whatsoever, whether it is accurate, or complete or otherwise and on express understanding that Sophos shall have no liability whatsoever to other parties in any way arising from or relating to the information or its use.
- Sophos SafeGuard PortProtector and Sophos SafeGuard PortAuditor are OEM versions of Safend Protector and Safend Auditor from Safend. Therefore some screenshots throughout this manual may still contain the Safend branding but mean the same as within the SafeGuard OEM version.

Boston, USA | Oxford, UK

© Copyright 2010. Sophos. All rights reserved. All trademarks are the property of their respective owners.

Other company and brand products and service names are trademarks or registered trademarks of their respective holders.

About This Guide

This user guide is comprised of the following chapters:

- ***Chapter 1, Introducing SafeGuard PortProtector,*** introduces the SafeGuard PortProtector solution, the system's architecture and how it works. It describes its features and benefits, in particular the new features in this version and provides a suggested workflow for using it to protect your organization's endpoints.
- ***Chapter 2, Getting Started,*** describes how to launch the SafeGuard PortProtector Management Console. It then provides a quick tour through the interface of the SafeGuard PortProtector Management Console and describes the Home World which provides access to the system's main functions.
- ***Chapter 3, Defining*** Policies**,** describes how to define SafeGuard PortProtector policies and how to manage them.
- ***Chapter 4, Distributing*** Policies**,** describes how to deploy SafeGuard PortProtector policies to the endpoints of your organization
- ***Chapter 5, Viewing Logs,*** describes how to monitor you organization by viewing logs derived from SafeGuard PortProtector Clients protecting your organization's endpoints, as well as logs derived from the SafeGuard PortProtector Server(s).
- ***Chapter 6, Managing Clients,*** explains how to view the status of the SafeGuard PortProtector Clients protecting your organization's endpoints and how to perform actions on these Clients, such as updating Client policies, reviewing latest Client information and more.
- ***Chapter 7, Administration,*** describes how to define global SafeGuard PortProtector administration settings.
- ***Chapter 8, End-User Experience,*** describes the experience of being protected by SafeGuard PortProtector Client (such as end-user messages) and the actions that can be performed in the Client, such as encrypting removable storage devices.
- ***Appendix A – Novell eDirectory Synchronization,*** explains how to synchronize SafeGuard PortProtector with Novell eDirectory
- ***Appendix B - Supported Device Types,*** lists the device models that SafeGuard PortProtector provides for your selection when building a policy.
- ***Appendix C – Supported File Types,*** lists the file types and extensions supported by SafeGuard PortProtector's File Type Control feature that provides control of files written to/read from storage devices.
- ***Appendix D – CD/DVD Media Scanner,*** describes how to scan and fingerprint specific CD/DVD media so that they can be approved for use in a white list.
- ***Appendix E - Using SafeGuard PortProtector in a HIPAA Regulated Organization***, provides guidance on how to address these threats within a HIPAA regulated environment.
- ***Appendix F – Using SafeGuard PortProtector in a SOX Regulated Organization,*** provides guidance on how to address these threats within a SOX 404 regulated environment.
- ***Appendix G – Using SafeGuard PortProtector in a PCI Regulated Organization,*** provides guidance on how to address these threats within a PCI DSS regulated environment.

- ***Appendix H - Using SafeGuard PortProtector in a FISMA Regulated Organization*** provides guidance on how to address these threats within a FISMA regulated environment.

Contents

1 Introducing SafeGuard PortProtector 6

2 Getting Started 22

3 Defining Policies 37

4 Distributing Policies 125

5 Viewing Logs 146

6 Managing Clients 194

7 Administration 216

8 End-User Experience 258

9 Appendix A – Novell eDirectory Synchronization 294

10 Appendix B - Supported Device Types 299

11 Appendix C – Supported File Types 301

12 Appendix D – CD/DVD Media Scanner 307

13 Appendix E - Using SafeGuard PortProtector in a HIPAA Regulated Organization 311

14 Appendix F – Using SafeGuard PortProtector in a SOX Regulated Organization 330

15 Appendix G – Using SafeGuard PortProtector in a PCI Regulated Organization 345

16 Appendix H – Using SafeGuard PortProtector in a FISMA Regulated Organization 359

1 Introducing SafeGuard PortProtector

About This Chapter

This chapter introduces the SafeGuard PortProtector solution, describes how it works and provides a suggested workflow for using it to protect your organization's data. It contains the following sections:

- ***The SafeGuard PortProtector Solution*** describes SafeGuard PortProtector's solution for providing enterprise-wide endpoint security by controlling and monitoring access to the ports and devices in an organization.
- ***SafeGuard Protection*** describes how SafeGuard PortProtector protects your ports and restricts the access of the devices and storage devices that connect through them.
- System Architecture describes the system's architecture and components.
- ***SafeGuard PortProtector Management Console*** describes the Management Console, which is a centralized tool for defining port protection policies for your organization, viewing logs and managing SafeGuard PortProtector Clients.
- ***SafeGuard Policy Enforcement – SafeGuard PortProtector Client*** describes SafeGuard PortProtector Client, which transparently runs on the endpoints in your organization and enforces the SafeGuard PortProtector protection policies on each machine on which it is applied.
- ***SafeGuard PortProtector Implementation*** Workflow describes the workflow for implementing and using SafeGuard PortProtector.

1.1 The SafeGuard PortProtector Solution

Together with SafeGuard PortAuditor (see the *SafeGuard PortAuditor User Guide*), SafeGuard PortProtector provides a comprehensive solution which enables organizations to see what ports and devices are being used in their organization (**visibility**), to define a policy that **controls** their usage and to **protect** data in motion.

SafeGuard PortProtector controls every endpoint and every device, over every network or interface. It monitors real-time traffic and applies customized, highly-granular security policies over all physical, wireless and storage device interfaces.

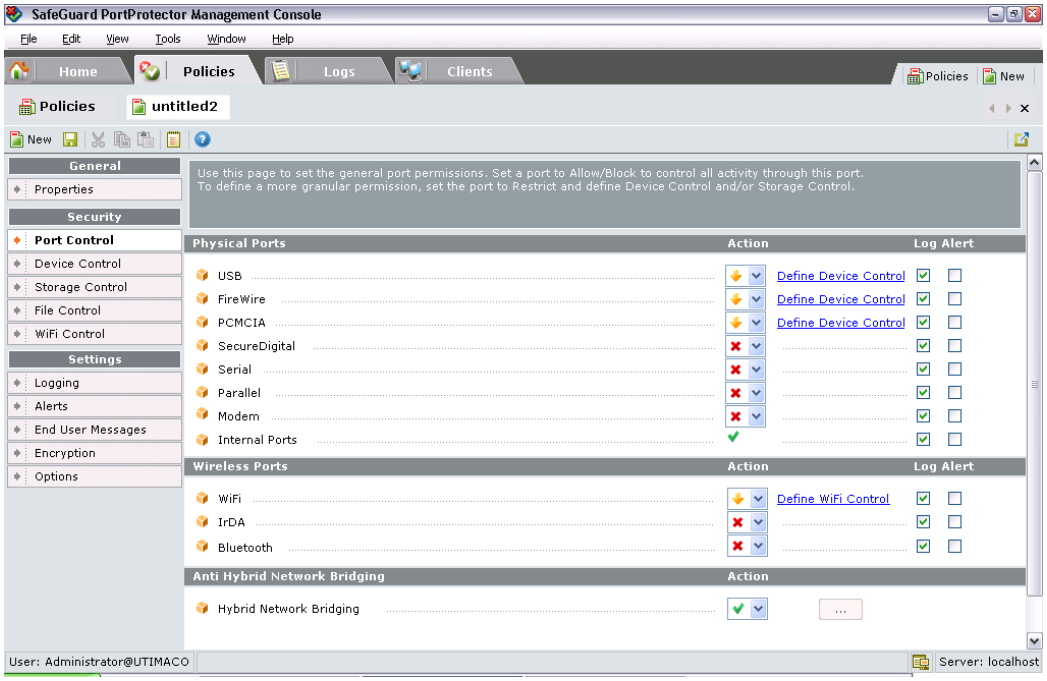
1.2 SafeGuard Protection

SafeGuard PortProtector protects your endpoints as follows:

1.2.1 Port Control

SafeGuard PortProtector can intelligently allow, block or restrict the usage of any or all computer ports in your organization according to the computer on which they are located, the user who is logged in and/or the type of port. SafeGuard PortProtector controls: USB, PCMCIA, FireWire, Secure Digital, Serial, Parallel, Modem (e.g. dialup, 3G etc.), WiFi, IrDA and Bluetooth ports.

A blocked port is unavailable, as if its wires were cut. An indication that a port is blocked is given when the computer boots or when a policy is applied that disables a previously allowed port.



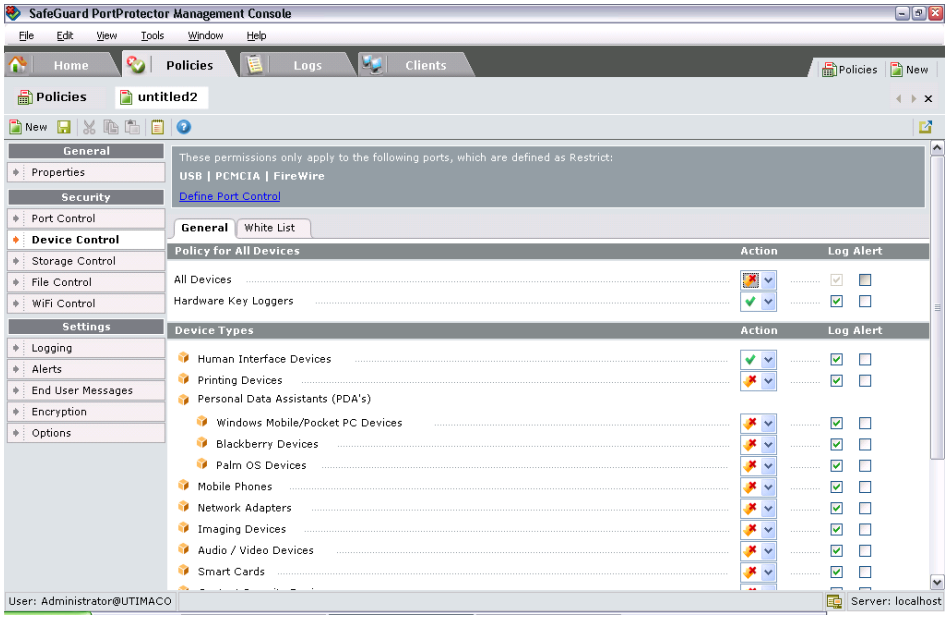
Further details about port control are provided in *Step 4: Define Port Control* in *Chapter 3, Defining Policies*.

1.2.2 Device Control

In addition to controlling port access, SafeGuard PortProtector provides another level of granularity by enabling you to define which devices can access a port.

For USB, PCMCIA, FireWire ports you can define which device types, device models and/or distinct devices can access a port, as follows:

- **Devices Types:** This option enables you to restrict access to a port according to the type of device that is connected to it. Examples of device types are printing devices, network adapters, human interface devices (such as a mouse) or imaging devices.
  The device types that are available for selection are built into SafeGuard PortProtector. If you would like to allow a device that is not of one of the types listed here, you can use the **Models** or the **Distinct Devices** option, described below.



- **Models:** This option refers to the model of a specific device type, such as all HP printers or all M-Systems disk-on-keys.
- **Distinct Devices:** This option refers to a list of distinct devices each with their own unique serial number, meaning each is an actual specific device. For example: the CEO's PDA may be allowed and all other PDAs may be blocked.

1.2.2.1 Protection against Hardware Key Loggers

Hardware Key Loggers are devices that can be placed by a hostile entity between a keyboard and its host computer in order to tap and record keyboard input and steal vital information, especially identity and password.

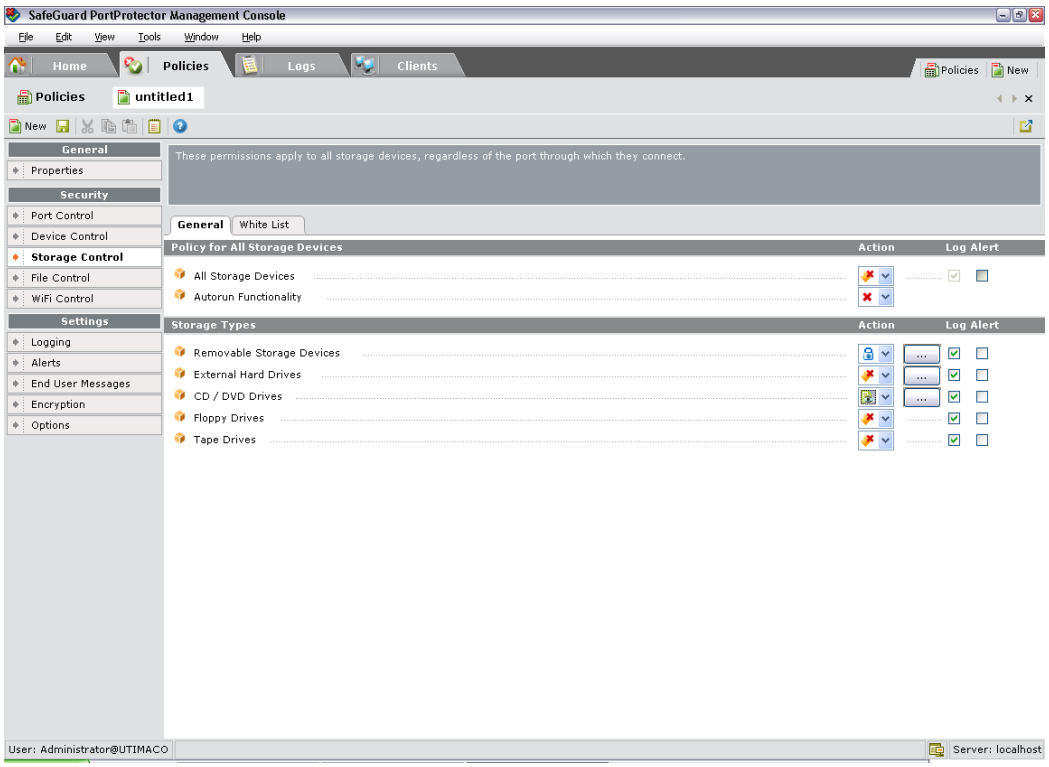
With SafeGuard PortProtector you can immunize your users against this threat: SafeGuard PortProtector can detect hardware key loggers connected to a USB or PS/2 port, and your policy can specify whether hardware key loggers should be blocked when detected.

Further details about device control are provided in *Step 5: Define Device Control* in *Chapter 3, Defining Policies*.

1.2.3 Storage Control

Storage control provides an additional level of detail in which to specify the security requirements of your organization. This can apply to all storage devices, internal or external, fixed or detachable. You can block storage devices completely, allow read-only access. You can also encrypt removable storage devices.

Similarly to non-storage devices, described in the previous section, storage devices can be also approved according to their type, model or distinct ID.



1.2.3.1 U3 Smart Drive and Autorun Control

Certain Disk On Key devices, such as U3 devices, offer smart functionality in addition to their basic storage functionality. This functionality allows them to store and run applications once connected to a host computer.

With SafeGuard PortProtector, you can let your end-users use their new sophisticated storage devices, while ensuring your endpoints are not exposed to potential exploits and risky applications these devices may carry as part of their U3 and smart storage capabilities. You can easily block both U3 and auto-launch activities as part of your security policy. Using our unique granular Client technology, you can still allow smart storage devices to be used as simple storage devices, so long as they comply with the rest of your storage policy, and block only their smart functionality which may be unsafe.

1.2.3.2 SafeGuard PortProtector Storage Encryption

SafeGuard PortProtector Media Encryption allows administrators to mandate the encryption of all the data being transferred off organization endpoints to approved removable media devices such as USB flash drives, Disk on Keys, memory sticks and SD cards, as well as CD/DVD and external Hard Disks. This provides organizations with comprehensive protection from both accidental data loss and deliberate leakage of corporate assets.

Unique to the SafeGuard PortProtector solution is the ability to restrict the usage of encrypted devices and media to company computers. This extends the security borders of organizations and prevents rogue employees from deliberately leaking data through these high-capacity devices.

Within the organization, media encryption is completely transparent. End-users are able to read and write to media just as they would normally do. However, when the same device or media is used on a computer that is not part of the organization, the data on it will not be accessible.

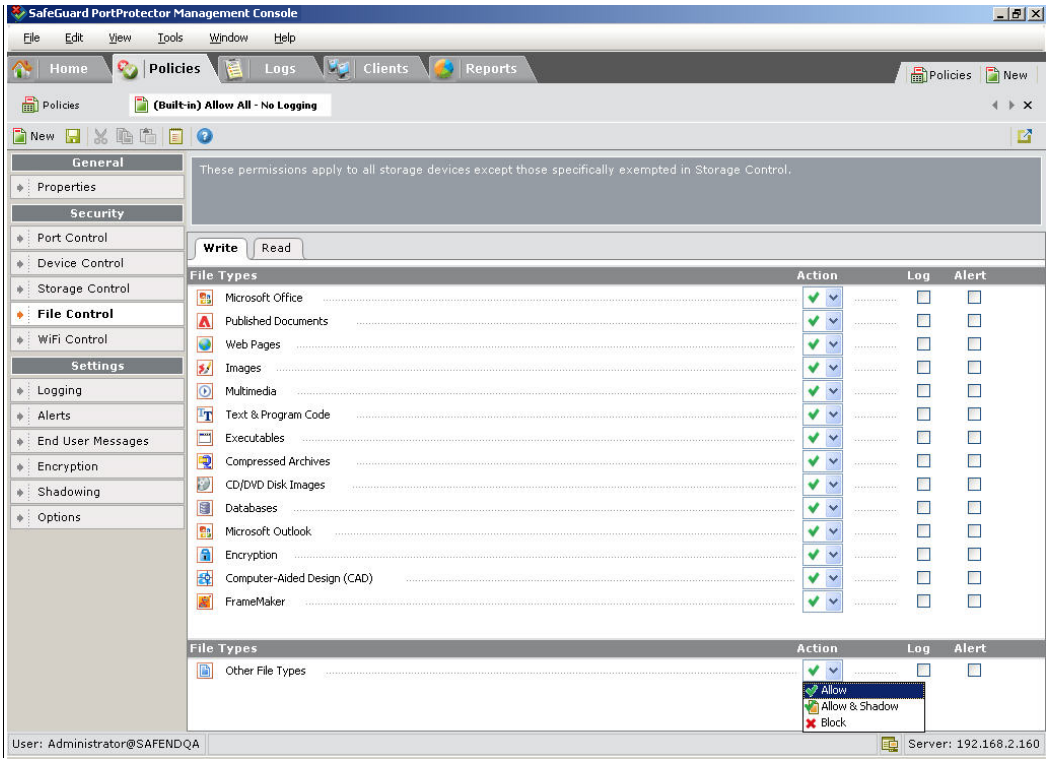
SafeGuard PortProtector Media Encryption is designed to work company-wide. Encrypted devices can be read and used interchangeably on any computer in the organization, while existing control based on device vendor/model and Serial Number still applies.

For removable storage devices, the SafeGuard PortProtector administrator can choose whether or not to allow specific users password-protected access to the data on non-authorized computers. If allowed, each user is able to set his/her own offline password, and use the Access Secure Data utility (which is found on the encrypted device) on a non-authorized computer to enter his/her password and access the data securely.

Further details about storage control are provided in *Step 6: Define Storage Control*Step 6: Define Storage Control in Chapter 3, Defining Policies.

1.2.4 File Control

File Control includes an additional layer of granularity and security by monitoring and controlling file transfers to/from external storage devices. Definitions are set on the level of file types providing the ability to allow or block specific file transfers as well as generating logs and alerts.



1.2.4.1 File Type Control

With File Type Control a highly reliable classification of files is performed by inspecting the file header contents rather than using file extensions, thus preventing users from easily bypassing the protection by renaming file extensions. With over 180 built-in file extensions covering all popular applications categorized into 14 file categories, policy definition has never been easier.

By inspecting both files downloaded to external storage devices and those uploaded to the protected endpoint, multiple benefits can be achieved:

- An additional protection layer for preventing data leakage
- Prevention of viruses/malware introduction via external storage devices
- Prevention of inappropriate content introduction via external storage devices. Examples of such content:
- Unlicensed software
- Unlicensed content (e.g. music and movies)
- Non work-related content (e.g. personal pictures)
- See *Step 7: Define File* Control in *Chapter 3, Defining policies* for further details.

1.2.4.2 File Logging and Shadowing

An additional level of monitoring the activity in your organization is provided in the File Logging feature, which enables you to log information written to or read from removable media devices or CD/DVD. File logs as well are viewed in the Logs World.

This option provides you with an audit trail of what data is transferred in and out of the organization, and may be used to analyze security incidents, as well as keep track over people's activity, and notice potential abuse of portable storage devices. It will help you better comply with security regulations you may be bound by, and will enhance your visibility into how your organizational data flows.

For highly sensitive sections of your organization, or for specific users who requires special attention, you can also use the File Shadowing feature. This feature allows you to collect copies of files moved to/from external storage devices. The files are stored in a central repository and can be viewed by authorized administrators. Please note - Since using this ability will influence both network utilization and storage resources you should use it with caution, preferably on small, well defined parts of your organization.

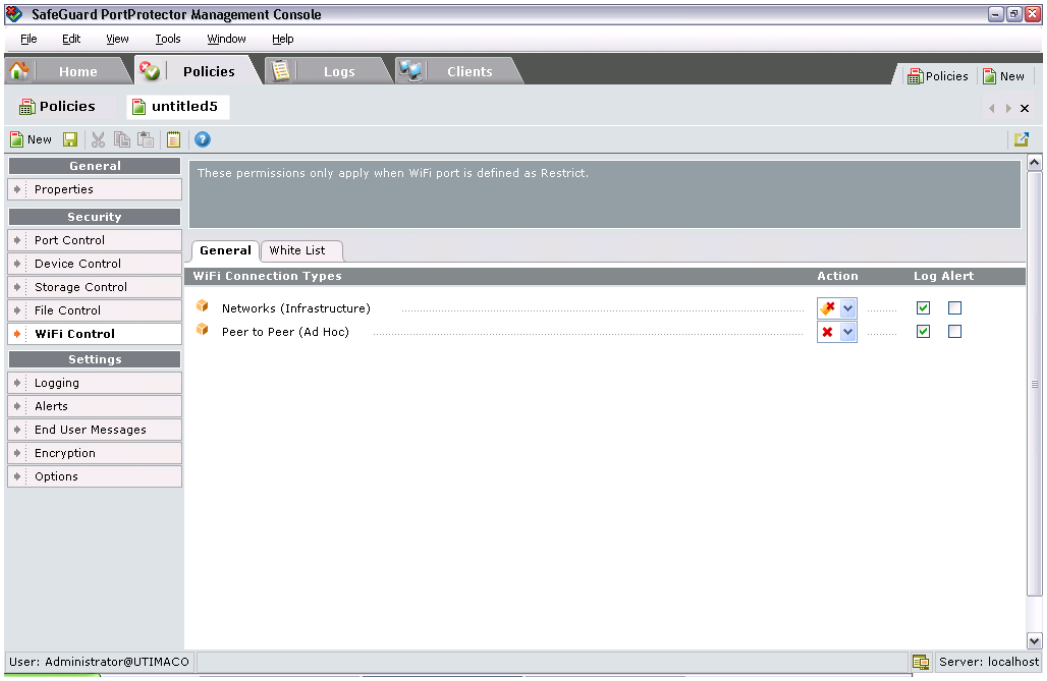
Using file name monitoring and file shadowing allows administrators the freedom to create policies that do not restrict usage of devices, yet allow full visibility of the activity and content transferred to removable media (for more details refer to Additional Permissions in *Chapter 3, Defining Policies*).

1.2.4.3 Content Inspection Integration

Administrators can also benefit from existing Content Monitoring and Filtering systems for controlling file transfers to external storage devices. With this technology, each file that is downloaded from an endpoint to an external storage device can be inspected to determine whether it contains sensitive information of any kind (e.g. intellectual property, consumer data etc.). Once it is determined that the file contains sensitive information, the user is notified that this file should not be transferred to external devices, and a trace log is created for the administrator. With this log, the administrator is provided a fine-grained list of data breaches through external storage devices.

1.2.5 WiFi Control

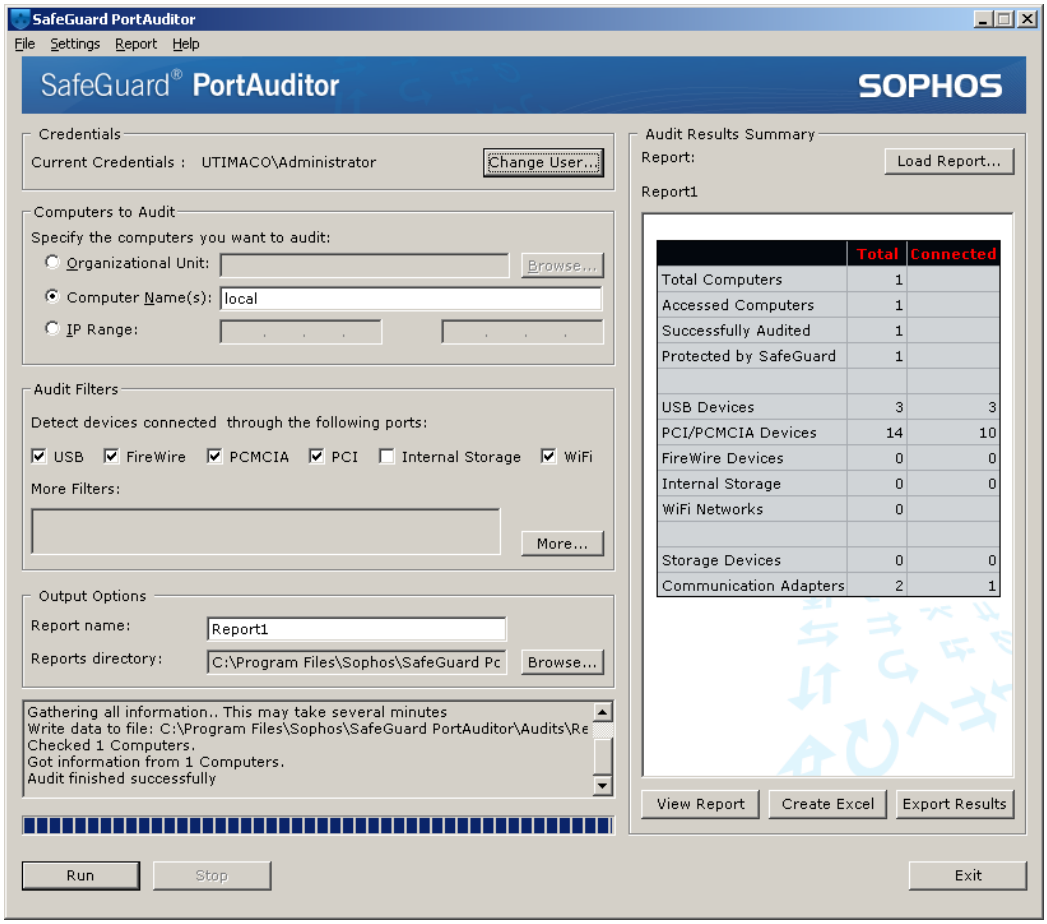
WiFi control ensures that users only connect to approved networks. You can specify which networks or ad hoc links are allowed access. You can specify the MAC address of the access points, SSID of the network, authentication method and encryption methods to define approved links.



More detail is provided in *Chapter 3, Defining Policies*.

1.2.6 SafeGuard PortAuditor

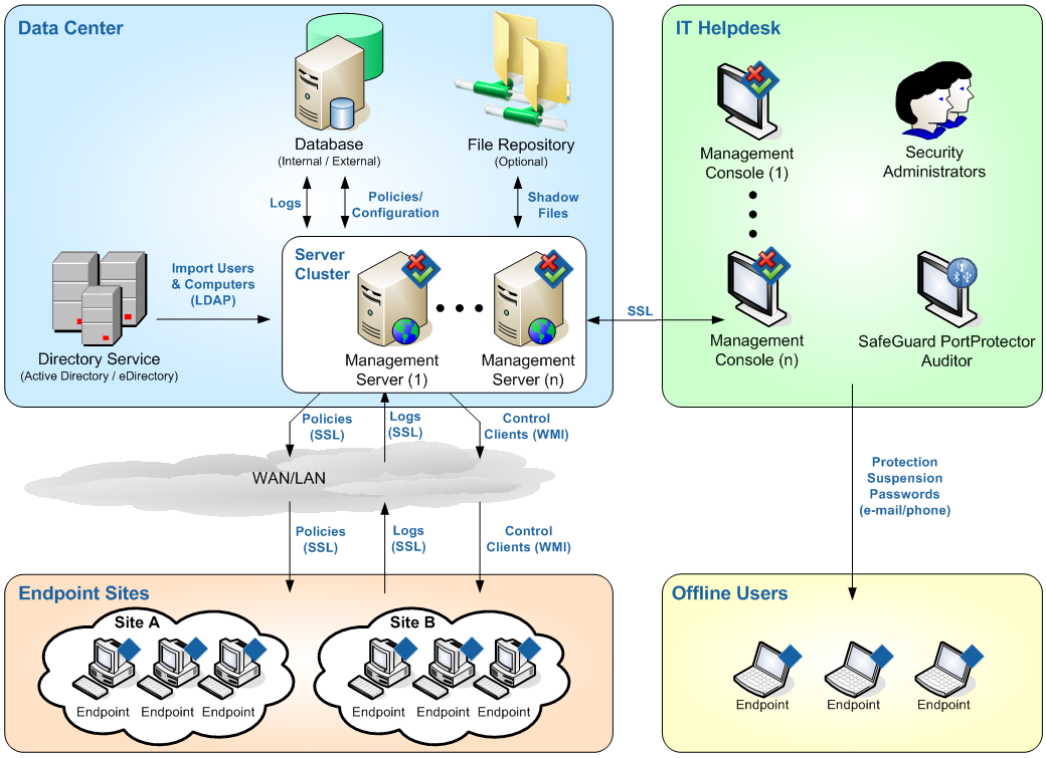
Although not an integral part of SafeGuard PortProtector, SafeGuard PortAuditor is a tool that goes hand in hand with SafeGuard PortProtector and completes it by providing you with a full view of what ports, devices and networks are (or were previously) in use by your organization's users. You use the output of a SafeGuard PortAuditor scan to select the devices and networks whose usage you want to approve.



More detail is provided in the *SafeGuard PortAuditor User Guide*.

1.3 System Architecture

The system architecture is described in the following figure:



The system comprises the following components:

- **SafeGuard PortProtector Management Server(s)** - SafeGuard PortProtector Management Server(s) store policies and other definitions, collect logs from Clients, enable Client management and distribute policies to Clients. The Management Server(s) uses either an internal/external database for its repository (see below).

  The Management Server(s) use IIS to communicate with Clients and Management Consoles (over SSL). Controlling Clients is performed via WMI. LDAP compliant protocols are used to synchronize with the existing organizational objects stored in Active Directory/Novell eDirectory.
  The Management Server(s) typically distribute policies directly to Clients (via SSL). It also supports an alternative distribution method which uses the Active Directory GPO mechanism. GPOs representing policies are written to Active Directory and after they are linked with the OUs of the organization, the policies are downloaded and applied to endpoints.

- **Internal/External Database** – Standard databases are used for storing system configuration, policies and log data. Administrators may opt to use an internal MySQL database supplied in the Management Server installation package or to connect to existing MSSQL database infrastructures. While using the internal database is simpler and maintenance free, connecting to an external database provides better performance and scalability. Note that server clustering is only possible using an external MSSQL database.

- **SafeGuard PortProtector Management Console** – enables you to manage Clients, view logs, define policies and administer the system. The Management Console can be installed and run from any computer on your network and uses SSL when communicating with the Management Server. The management console supports one-click deployment from the server website.
- **SafeGuard PortProtector Client** - protects and monitors the endpoints in your organization, and alerts/reports about port activity. The Client communicates with a SafeGuard PortProtector Management Server using SSL.
- **SafeGuard PortAuditor** - Although not an integral part of SafeGuard PortProtector, SafeGuard PortAuditor is a light-weight client-less tool that goes hand in hand with SafeGuard PortProtector and completes it by providing you with a full view of what ports, devices and networks are (or were previously) in use by your organization's users. You use the output of a SafeGuard PortAuditor scan to select the devices and networks whose usage you want to approve.
- **SafeGuard PortProtector Management Server Cluster** - A server cluster enables the installation of several SafeGuard PortProtector Management Servers connected to a single external database, so that they seamlessly share the load of traffic from the endpoints, as well as to provide redundancy and high availability.
- A server cluster can only be created on systems using an external MSSQL database (not an internal database), which can be accessible to all the member servers of the cluster. These servers share a single MSSQL database or an MSSQL database cluster.
- The list of available servers is routinely transferred to clients. Clients randomly select the server with which to connect in order to ensure an even distribution of the load between servers. In case of a failure to connect to a specific server, the client will immediately select another server and connect to it.
- **Note:** Management consoles will connect to the server from which they were originally installed.

1.4 SafeGuard PortProtector Management Console

SafeGuard PortProtector's Management Console is a unified management tool to be used by your IT and/or security departments for defining permissions through policies, manage Clients and monitor port, device and network usage in your organization.

1.4.1 How Does It Work?

The Management Console integrates with your Active Directory or Novell eDirectory so you can easily associate policies with your network computers and users. Distribution of policies is typically performed directly from the server(s) to the endpoints (via SSL). Other options include the well-proven Group Policy mechanisms of Active Directory, or any third-party tools you may use in your network.

The SafeGuard PortProtector Management Console is automatically installed on the same machine as your SafeGuard PortProtector Management Server during Server installation, and can be installed on additional computers as needed.

You can then define policies as described in *Chapter 3*, *Defining Policies.*

After the policies are distributed and applied to endpoints, you can view the log records in the Logs World, as described in *Chapter 5, Viewing Logs*.

1.4.2 Policy Definition

1.4.2.1 What Does a Policy Define?

Each policy defines two types of information: **Security** definitions and policy **Settings**, as follows.

- **Security** definitions specify the policy (blocked, allowed or restricted) for accessing the ports on your organization's endpoints:
- **Port Control** specifies your organization's policy regarding port access on endpoints.
- **Device Control** specifies your organization's policy regarding the devices that are allowed to access USB, PCMCIA and FireWire ports on endpoints.
- **Storage Control** specifies your organization's policy regarding the storage devices that are allowed to access USB, PCMCIA and FireWire ports on the endpoints (includes encryption of removable storage devices).
- **File Control** specifies your organization’s policy regarding files transferred to/from external storage devices. This controls transfers by file type as well as actual content.
- **WiFi Control** specifies your organization's policy regarding the WiFi links that endpoints are allowed to access.
- **Settings** specify how the policy behaves on the endpoint:
- **Logging** specifies the logging settings for the policy, such as the frequency for sending log entries to a SafeGuard PortProtector Management Server from a protected endpoint.
- **Alerts** selects the destinations to which alerts for the policy should be sent.

- **End-user Messages** enables you to edit the default messages that appear on a protected endpoint during ongoing usage and when a policy violation occurs.
- **Media Encryption** determines the system's behavior when removable storage device permissions require encryption.
- **Content Inspection** (available only if Content Inspection is activated) defines the settings required when using content inspection. Such as alert sending setting, file cache size and more.
- **Options** enable you to define various behavioral aspects of the policy, such as how it disconnects active devices when the need arises.

All of the above are described in detail in *Chapter 3, Defining Policies.*

1.4.2.2 How Do You Define a Policy?

SafeGuard PortProtector Policies are defined in the SafeGuard PortProtector Management Console. You can define one policy for your entire organization, or define customized policies for each organizational unit (computers and/or users) defined in your Active Directory or Novell eDirectory.

Policies need to be defined once and then updated on an as-needed basis when the need arises in your organization. To define a new policy, simply define each of the policy aspects described above and save the policy.

Chapter 4, Distributing Policies describes the options for distributing policies directly from the server(s), via Microsoft's Active Directory GPO or through registry files.

Once you have defined and distributed a policy to SafeGuard PortProtector Clients you can view activity logs from each client through the Logs World in the SafeGuard PortProtector Management Console, described in *Chapter 5, Viewing Logs*. Log entries include a variety of information, such as:

- policy violations, such as an attempt to use a blocked device
- the use of read-only storage devices
- the distribution of new policies

After analyzing the logs, you may wish to adjust your policies. You may refer to *Chapter 3, Defining Policies* for a detailed explanation of how to define policies.

1.5 SafeGuard Policy Enforcement – SafeGuard PortProtector Client

SafeGuard PortProtector Client constantly ***monitors*** real-time traffic on protected ports and applies customized, highly-granular security policies over all physical, wireless and removable storage interfaces. It ***blocks*** unauthorized activities (such as plug device, write to storage, connect to WiFi networks), ***protects*** data written to storage devices, ***alerts*** administrators about unauthorized usage attempts and ***logs*** events for future viewing and analysis.

SafeGuard PortProtector Client is a lightweight software package that transparently runs on endpoint computers, at kernel level, and enforces protection policies on each machine on which it is applied. It has a minimal footprint (in terms of file size, CPU and memory resources) and includes redundant, multi-tiered anti-tampering features to guarantee permanent control over endpoints.

SafeGuard PortProtector Client can be silently installed on all endpoints.

Policy distribution to endpoint computers can be handled either by the Management Server via SSL, or by using Microsoft's Active Directory's Group Policy Management Console or using any third-party tool that your organization has for distributing software.

Once policies have been distributed, the Client immediately starts protecting the ports of that computer without requiring a reboot.

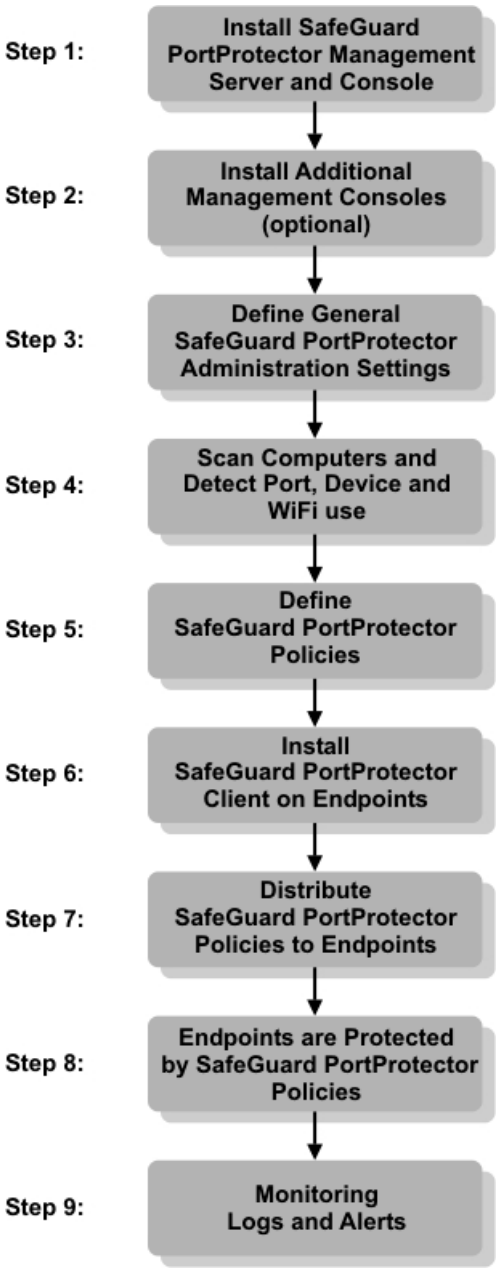
When a violation of a SafeGuard PortProtector policy occurs or during certain usage activities, a message is displayed on the endpoint computer. A policy violation means that someone has tried to use a port, device or WiFi link that was blocked on a computer on which SafeGuard PortProtector is applied. The end-user can simply click to acknowledge that the messages were read. A log entry may be created to record this event, according to the preferences you defined in your policy.

If you wish, you may install the Client in Stealth Mode, hiding both SafeGuard tray icon and messages and making SafeGuard PortProtector Client invisible to the user at the endpoint.

You may refer to chapter *End-User Experience* for more information.

1.6 SafeGuard PortProtector Implementation Workflow

The following is an overview of the workflow for implementing and using SafeGuard PortProtector.


Step 1:
Install SafeGuard PortProtector Management Server and Console
Step 2:
Install Additional Management Consoles (optional)
Step 3:
Define General SafeGuard PortProtector Administration Settings
Step 4:
Scan Computers and Detect Port, Device and WiFi use
Step 5:
Define SafeGuard PortProtector Policies
Step 6:
Install SafeGuard PortProtector Client on Endpoints
Step 7:
Distribute SafeGuard PortProtector Policies to Endpoints
Step 8:
Endpoints are Protected by SafeGuard PortProtector Policies
Step 9:
Monitoring Logs and Alerts

- Step 1: Install the SafeGuard PortProtector Management Server and Console, as described in the *SafeGuard PortProtector Installation Guide*.
- **Step 2: Install Additional Management Consoles**, as described in the *SafeGuard PortProtector Installation Guide*.
- **Step 3: Define General SafeGuard PortProtector Administration Settings,** such as the method in which policies are published, as described in *Chapter 7,* Administration.
- **Step 4: Scan Computers and Detect Port/Device Usage**. Use SafeGuard PortAuditor to detect the ports that have been used in your organization and the devices and WiFi networks that are or were connected to these ports, as described in the *SafeGuard PortAuditor User Guide*.
- **Step 5: Define SafeGuard PortProtector Policies.** In this stage you define the blocked, allowed and restricted ports, devices and WiFi networks according to the security and productivity requirements of your organization as described in *Chapter 3, Defining Policies*.
- **Step 6: Install SafeGuard PortProtector Client on Endpoints,** as described in the *SafeGuard PortProtector Installation Guide*.
- **Step 7: Distribute SafeGuard PortProtector Policies to Endpoints:** in this stage, you can either associate policies to users and computer and distribute directly to endpoints (via SSL), or use Active Directory's GPO feature to distribute SafeGuard PortProtector Policies or any other third-party tool, as described in *Chapter 4, Distributing Policies*.
- **Step 8: Endpoints are Protected by SafeGuard PortProtector Policies**: in this stage, only approved devices and WiFi networks can be used, through permitted ports. Logs about port, device and WiFi network use and attempted use, as well as tampering attempts, are created and sent to the Management Server as described in *Chapter 9, End-User* Experience.
- **Step 9: Monitoring Logs and Alerts,** view and export the log entries generated by SafeGuard PortProtector Clients, as described in *Chapter 5, Viewing Logs*.

2 Getting Started

About This Chapter

This chapter first describes how to launch the SafeGuard PortProtector Management Console. It then provides a quick tour through the interface of the SafeGuard PortProtector Management Console by describing its main windows and menus, and the *Home* tab window, or World. It contains the following sections:

- ***Launching SafeGuard PortProtector Management Console*** describes how to launch the Management Console.***Know*** Your Way around the Application describes the main sections and buttons in the application.
- ***Worlds*** describes the main tabs, each dealing with a different aspect of the application.
- ***Menu Bar*** describes the menu options available in the SafeGuard PortProtector Management Console.Window Bar and Window Options describes this special bar which is available in some of the application's windows, as well as its controls. It also describes functions available in some windows, such as duplicating and undocking a window.
- ***Home World*** describes the initial window of the SafeGuard PortProtector Management Console.

2.1 Launching SafeGuard PortProtector Management Console

Launch SafeGuard PortProtector Management Console as follows.

To log in:

Click the icon on your desktop,

OR

Select Start → Programs → SafeGuard PortProtector → Management Console. The following window opens:

1 Type in your User name, Password and Domain.

2 Click **Login**.

3 If you have acquired your permanent license and have not yet changed the default global uninstall password for SafeGuard PortProtector Clients, you will be prompted to do so in the following window that will appear:

Password Change Required
You are still using the default global uninstall password or the default global administration password for SafeGuard PortProtector Clients ('Password1').
It is highly recommended that you change this password now (Tools -> Global Policy Settings).
OK

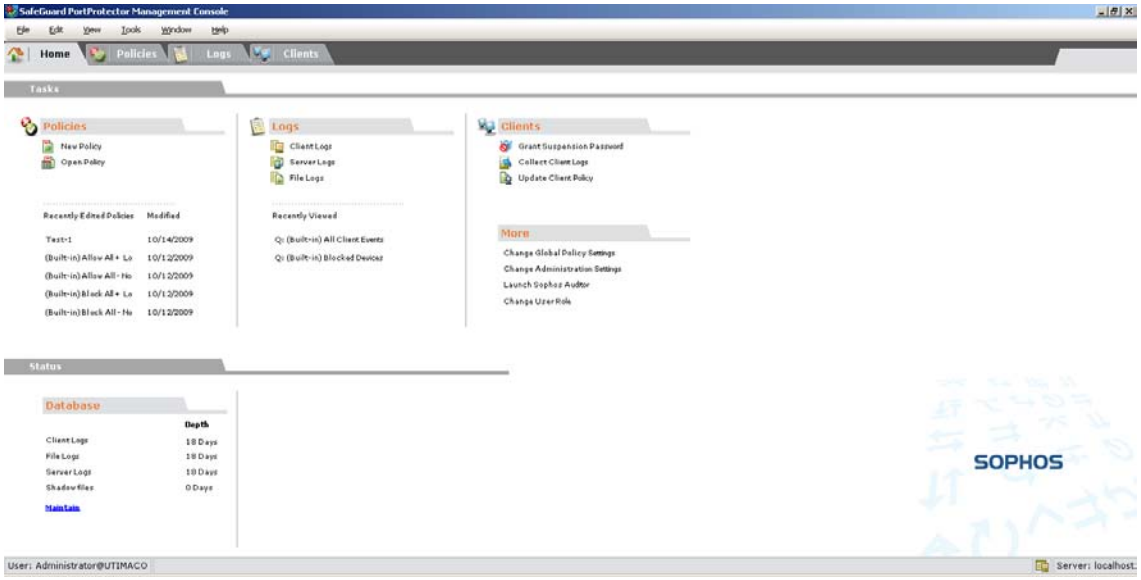
4 Click **OK**. The application opens, displaying the main window.

Note: A SafeGuard PortProtector administrator can be assigned more than one role in order to define the various domain partitions for which they are responsible. After such an administrator logs in, a selection window is automatically displayed for selecting the role in which to work. A

User Role defines the functions, OUs and domains of an organization to which a SafeGuard PortProtector administrator has access, as described in *Defining Roles*.

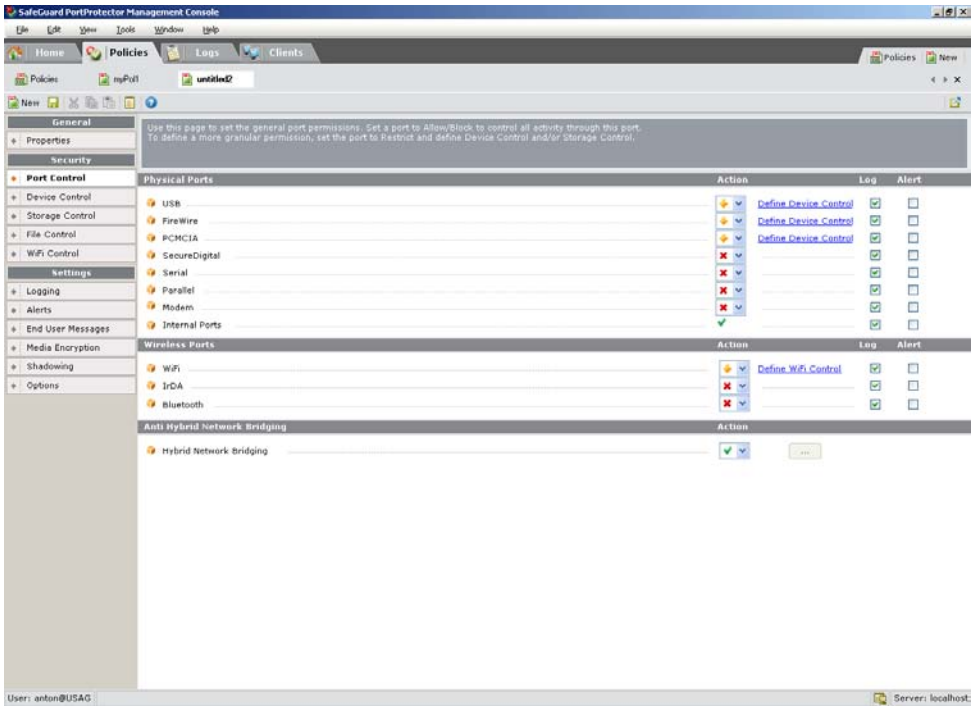
2.2 Know Your Way around the Application

After logging into the SafeGuard PortProtector Management Console, the following window is displayed:



This is the Home tab. It displays the Home World, which is explained in *Home World*.

Since this is not a typical window, please switch to the Policies tab. The following window opens:



The window includes the following areas:

- Worlds Tabs – each tab, or World, deals with a different aspect of the application (see *Worlds*).
- Menu Bar – displays the menus.
- Window Bar – displays the names of open windows in the Policies World and Logs World.
- Control Buttons – simplify launching and handling of windows in the Policies World and Logs World.
- Workspace – the workspace provides different information and options, depending on the active World. These are described in later chapters. The Home World, which is the initial World displayed when you launch SafeGuard PortProtector Management Console, is described in *Home World*

SafeGuard PortProtector Management Console is made up of four tabs. Each tab, or World, manages a different aspect of the application, as follows:

- **Home** – this World, discussed in *Home World*, provides an overview of the most common tasks and information available in the other Worlds, and is a central location from which you can activate these tasks and access the information.
- **Policies** – this World, discussed *in Chapter 3, Defining Policies*, is where you define and manage policies, including port, device and WiFi permissions, approved devices and networks (white lists), removable storage device encryption and more.
- **Logs** – this World, discussed in *Chapter 5, Viewing Logs*, is where you query, view and manage logs sent from protected Clients.
- **Clients** – this World, discussed in *Chapter 6, Managing Clients*, is where you view Client properties and status, update Client policies, generate a Client suspension password and more.

2.3 Worlds

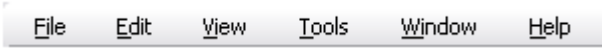
SafeGuard PortProtector Management Console is made up of four tabs. Each tab, or World, manages a different aspect of the application, as follows:

- Home – this World, discussed in Home World, provides an overview of the most common tasks and information available in the other Worlds, and is a central location from which you can activate these tasks and access the information.
- Policies – this World, discussed in Chapter 3, Defining Policies, is where you define and manage policies, including port, device and WiFi permissions, approved devices and networks (white lists), removable storage device encryption and more.
- Logs – this World, discussed in Chapter 5, Viewing Logs, is where you query, view and manage logs sent from protected Clients.
- Clients – this World, discussed in Chapter 6, Managing Clients, is where you view Client properties and status, update Client policies, generate a Client suspension password and more.

2.4 Menu Bar

Some of the menus in the SafeGuard PortProtector Management Console are common to all Worlds (*Edit*, *Tools* and *Window* menus), whereas others differ. The common menus will be described here, as well as the menus particular to the Home World.

The menu bar contains the following options:



2.4.1 File Menu

The *File* menu in the Home World enables you to open new Policy windows, Log windows, Reports, to log out of the Management Console and to Exit the application.

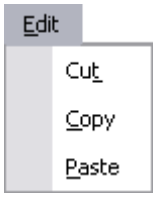
The *File* menu includes the following options:

Option	Description
New	Opens a submenu that enables you to open a new policy window, a new Clients Log window, a new Server Log window, a new File Log window or a new report.

Option	Description
Change User Role	A SafeGuard PortProtector administrator can be assigned more than one role in order to define the various domain partitions for which they are responsible. After such an administrator logs in, a selection window is automatically displayed for selecting the role in which to work. **Note:** A User Role defines the functions, OUs and domains of an organization to which a SafeGuard PortProtector administrator has access, as described in *Defining Roles*. The **Change User Role** option enables such an administrator to change this role at any time to another role that has been assigned to him or her.
Logout	Logs the current user out of the Management Console.
Exit	Logs out the current user and closes SafeGuard PortProtector Management Console

2.4.2 Edit Menu

The *Edit* menu is common to all Worlds, although menu items are disabled in all but the Policies World. It provides **Cut**, **Copy** and **Paste** options for the **Add Device, Add Storage Device** or **Add WiFi Network** option, which is described in *Approving Devices and WiFi Connections* in *Chapter 3, Defining Policies*.

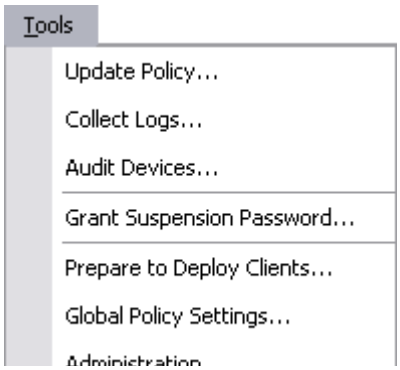


2.4.3 View Menu

The *View* menu in the Home World enables you to view the progress of Client tasks. Refer to *Tracking Client Task Progress* in *Chapter 6, Managing Clients* to learn about Client tasks.

2.4.4 Tools Menu

The *Tools* menu is common to all Worlds. It enables you to perform various management and administration tasks.



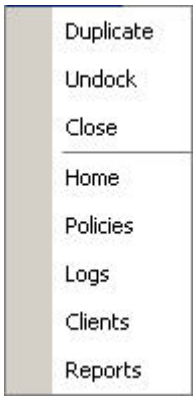
The *Tools* menu includes the following options:

Option	Description
Update Policy	Updates policies (for details see in *Chapter 6, Managing Clients*).
Collect Logs	Collects logs (for details see *Retrieving Latest Information from a Client* in *Chapter 6, Managing Clients)*. **Note:** This option can also be accessed by right-clicking on this client in the Clients World.
Audit Devices	Launches SafeGuard PortAuditor
Grant Suspension Password	Creates a key that can be used to grant a suspension key to a user in order to temporarily suspend protection (for details *Temporary Suspension of SafeGuard Protection* see in *Chapter 6, Managing Clients)*. **Note:** This option can also be accessed by right-clicking on this client in the Clients World.
Prepare to Deploy Clients	Explains what needs to be done in order to deploy Clients and points to location of installation files

Option	Description
Global Policy Settings	Enables viewing and modifying of Global Policy Settings (for details see *Step 9: Define Global Policy Settings* in *Chapter 3, Defining Policies*). **Note:** This option can also be accessed by right-clicking on this client in the Clients World.
Administration	Enables administrator to perform administrative tasks (for details see *Administration Window* in *Chapter 7, Administration*).

2.4.5 Window Menu

The *Window* menu is common to all Worlds. It enables you to switch to other Worlds, open additional windows, as well as to duplicate, undock and close windows in the Policies World and the Logs World (these options are explained in *Window* Bar and Window Options).



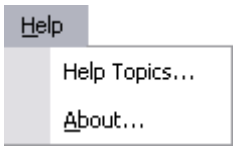
The *Window* menu includes the following options:

Option	Description
Duplicate	Duplicates the active window. Enabled in the Policies and the Logs worlds only.
Undock	Undocks the active window. Enabled in the Policies and the Logs worlds only.
Close	Closes the active window. Enabled in the Policies and the Logs worlds only.
Home	Opens the Home world.
Policies	Opens the Policies world.

Option	Description
Logs	Opens the Logs world.
Clients	Opens the Clients world.
Reports	Opens the Reports world.

2.4.6 Help Menu

The *Help* menu provides information describing SafeGuard PortProtector.



The *Help* menu is common to all the Worlds and includes the following options:

Option	Description
Help Topics	Opens the SafeGuard PortProtector Policy Builder help.
About	Displays copyright and licensing information about SafeGuard PortProtector, as well as contact information.

SafeGuard PortProtector™ Management Console - About
SafeGuard® PortProtector
SafeGuard PortProtector™ Management Console
Version: 3.3 (build 55031.46115)
Copyright of Sophos Plc All rights reserved.
Website: www.sophos.com
Support: support@sophos.com
Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this product or any portion of it may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.
SOPHOS

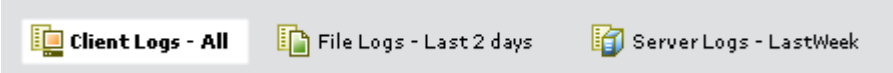
2.5 Window Bar and Window Options

In the Policies World and in the Logs World, multiple windows may be opened. The Window bar displays open windows.

2.5.1 Window Bar

In the Policies World, in addition to the main window from which you manage policies you can open several policies, each in a separate window. The Window Bar displays the names of open policies:

In the Logs World, you can open several logs, each in a separate window. The Window Bar displays the names of open log queries:



2.5.2 Control Buttons

To help you open, manage and navigate windows in the Policies World the Logs world, several control buttons are available. These buttons appear on the top right-hand side of each window.

- **Launch buttons**

, top right-hand side of the Policies or Logs window – these buttons allow you to open additional windows easily. Launch buttons differ in the Policies World and in the Logs World and are explained in their respective chapters.
- **Navigation buttons** - the left and right arrows enable you to display additional open windows when more windows are open than can be viewed in the Windows bar.
- **Close button** next to the navigation buttons - use this button to close the active window (the active window is the currently displayed window whose name is highlighted in the Window bar).
- **Undock button** - use this button to undock the active window (the active window is the currently displayed window whose name is highlighted in the Window bar). For an explanation of window undocking refer to *Undocking and Docking a Window*.
- **Dock button** – when a window has been undocked the **Dock** button appears instead of the **Undock** button. Click it in order to dock the window back into its World. For an explanation of window undocking refer to *Undocking and Docking a Window*.

2.5.3 Active Window Options

The active window is the window which is currently displayed and whose name is highlighted in the Window bar. The active policy window in the Policies World and the active log window in the Logs World can be duplicated, undocked and closed.

2.5.3.1 Duplicating a Window

You may wish to duplicate a window, for example in the Policies World in order to use a policy as a starting point for another policy, or in the Logs World, in order to apply the same query to different Organizational Tree items.

To duplicate the selected window:

From the *Window* menu, click **Duplicate**.

OR

1 In the Window bar, right-click the name of the window you wish to duplicate. The selected window becomes active and a menu opens.

2 From the menu, click **Duplicate Window**.

A new Log window opens which is identical to the displayed window.

2.5.3.2 Undocking and Docking a Window

Undocking a window makes the window separate and independent of its World tab. This is useful when you would like to switch to another World, but still keep the active window open.

To undock the active window:

From the *Window* menu, click **Undock**.

OR

In the top right-hand side of the active window, click the **Undock** button.

OR

In the Window bar, right-click the name of the window you wish to duplicate. The selected window becomes active and a menu opens.

From the menu, click **Undock Window**. The active window is now separate and independent.

If you wish, you can dock an undocked window back into its World.

To dock an undocked window:

In the top right-hand side of the undocked window, click the **Dock** button. The window is docked back into its World.

2.5.3.3 Closing a Window

To close the active window:

Click the **Close** button situated on the top right corner of the window.

OR

1 In the Window bar, right-click the name of the window you wish to close. The selected window becomes active and a menu opens.

2 From the menu, click **Close Window**.

The window closes.

2.5.3.4 Navigating Between Open Windows

There may be cases in which more windows are open than can be viewed in the *Window* bar. You can navigate right or left in order to reach the required window.

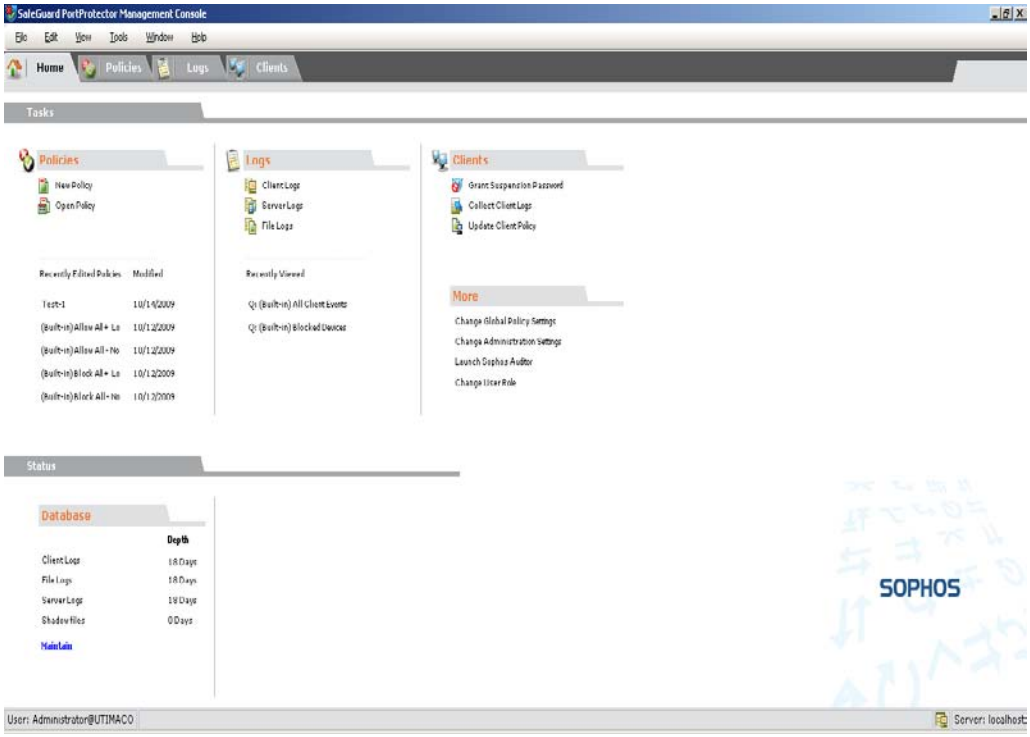
To navigate between open windows:

Click the right or left arrows situated on the top right corner of the window until the required window is viewable in the Window bar.

2.6 Home World

The Home World provides a central access point to the most common tasks and recent information from the other worlds.

> **Note:** A general description of the tasks and information types which can be accessed from the Home World is provided here. To learn more about each task/information type please read the relevant chapter in this user manual.



2.6.1 Home World – Description

The workspace is divided into two areas: Tasks and Status.

Tasks

This area, in the top half of the window, contains links and tool buttons to access information and major functions from other Worlds. These functions can all be performed from each World using menus, toolbar buttons and/or right-click menus. The area is divided into four sections, as described below:

- **Policies:** Clicking the section heading switches to the Policies World. This section includes icons and links to the following:
- **New Policy** – click to define a new policy.
- **Open Policy** - click to open an existing policy. The Policy Management window opens.
- **Recently Edited Policies** – for your convenience, a list of the last five policies that were edited is provided, along with the modification date. Click the required policy to open it. Refer to *Chapter 3, Defining Policies* for a detailed explanation of policy definition and management.
- **Logs and Reports:** Clicking the section heading switches to the Logs World. This section includes icons and links to the following:

- **Open Report** – click to open the SafeGuard PortProtector reports. You may refer to *Chapter 7,* for a detailed explanation of SafeGuard PortProtector's Reports world.
- **Client Logs** - click to view logs and alerts from protected Clients.
- **Server Logs** - click to view SafeGuard PortProtector Server logs.
- **File Logs** - click to view logs which track files written to or read from protected Clients.
- **Recently Viewed** – for your convenience, a list of the recently viewed queries and reports (not including untitled queries) is provided. Click to run the desired query or report. Queries are indicated by a **Q:** prefix and reports by a **R:** prefix.

  Refer to Chapter 5, Viewing Logs for a detailed explanation of logs, queries and log management.
- **Clients:** Clicking the section heading switches to the Clients World. This section includes icons and links to the following:
- **Grant Suspension Password** – click to grant a suspension password for a Client. This enables you to temporarily suspend protection on the Client without having to uninstall the SafeGuard PortProtector Client.
- **Collect Client Logs** – click to collect logs from protected Clients immediately, without having to wait for the log transfer interval to complete.
- **Update Client Policy** – click to update policies on Clients immediately, without having to wait for the predefined update interval to complete.
  Refer to Chapter 6, Managing Clients for a detailed explanation of Client management.
- **More:** This section includes icons and links to the following:
- **Change Global Policy Settings** – click to open the Global Policy Settings window in order to change the Global Policy settings. These are the default settings for all policies unless policy specific settings have been defined. Refer to *Step 9: Define Global Policy Settings* in *Chapter 3, Defining Policies* for a detailed explanation.
- **Change Administration Settings** – click to open the Administration window in order to change administration settings. Refer to *Chapter 7,* Administration for a detailed explanation.
- **Launch SafeGuard PortAuditor** – click to open the Path to SafeGuard PortAuditor window in order to launch SafeGuard PortAuditor and scan your organizational network and detect currently and previously connected devices and WiFi links. Refer to SafeGuard PortAuditor User Guide for a detailed explanation.

Status

This area on the bottom half of the window displays information about your SafeGuard PortProtector database and license. The area is divided into two sections, as described below:

- **Database** – for each log type (Client, File, Server) the number of stored days is displayed. Clicking the **Maintain** link or the section heading switches to the *Database Management* window so that you can change depth settings and other settings if you so wish. In case of an emergency purge of database records (see *Defining Database Maintenance Settings* in *Chapter 7, Administration)*, a message appears in this section.

Task Bar

The task bar at the bottom of the Home World as well as all other worlds displays the name of the administrator currently logged in and the name of the SafeGuard PortProtector Management Server.

3 Defining Policies

About This Chapter

This chapter describes how to build and manage SafeGuard PortProtector policies in the Policies World and contains the following sections:

- ***What is a Policy*** describes what a policy is and how it protects your endpoints.
- ***Quick Tour of the Policies World*** describes the Policies World window.
- ***Defining SafeGuard PortProtector Policies - Workflow*** provides an overview of the workflow for defining a new policy. It suggests a simple and straightforward process for performing these steps, from which you may deviate, if you prefer. A reference is provided from each of these steps to a sub-section that describes it in detail.
- ***Approving Devices and WiFi Connections*** describes how the *Device Control* window, *Storage Control* window and *WiFi Control* window enable you to define groups of device models, groups of distinct devices and groups of WiFi networks, and their access permissions to the ports that are allowed in the *Port Control* window.
- ***Approving CD/DVD Media*** describes how to allow the use of fingerprinted CD/DVD media by adding them to a White List.
- ***Managing Policies*** explains how to perform actions such as saving and publishing a policy, exporting and importing policies, deleting policies and more.
- ***Active Window Options*** discusses duplicating, undocking and closing a window.

3.1 What is a Policy

A SafeGuard PortProtector policy defines how you want to protect access through the ports of the endpoints belonging to a specified organizational unit (OU, group of computers or users). The entire set of SafeGuard PortProtector policies and their assignment to the OUs of your organization determine your organization's protection policy.

A SafeGuard PortProtector policy specifies which ports are allowed, blocked or restricted. **Restricted** means that only specified device types, device models, distinct devices or WiFi connections can gain access through this port.

A policy specifies the access permissions of storage device types, storage device models and distinct storage devices, as well as WiFi connections, enabling you to specify whether they are allowed, blocked, restricted (in the same manner as for devices), or allowed Read Only access.

A policy can also block **Hardware Key Loggers** that are connected to a USB or a PS/2 port. Hardware Key Loggers are devices that can be placed by a hostile entity between a keyboard and its host computer in order to log keyboard input. Your policy can specify whether hardware key loggers should be blocked when detected by SafeGuard PortProtector.

For each port, device, storage device and WiFi connection, SafeGuard PortProtector policies also define whether its activities (such as connection or disconnection of a device) are logged, and whether these activities trigger an alert. Logs and alerts are encrypted, stored on the SafeGuard PortProtector Management Server, and can be viewed in the Logs World, described in *Chapter 5, Viewing Logs*. Alerts are sent immediately to predefined destinations and can also be viewed in the Logs World.

An additional level of monitoring the activity in your organization is provided in the File Type Control, which enables you to control and alert/log or save a hidden copy of files written to or read from removable media devices or CD/DVD. File logs as well can be viewed in the Logs World.

When integrated with a third-party content inspection solution, files transferred to storage devices can be set to be inspected prior to their transfer.

A policy can be set to require that removable media devices, including CD/DVD media and external hard disks attached to a computer protected by this policy be encrypted, so that only devices encrypted by the organization can be used. Devices encrypted by the organization can only be used by organizational computers, thereby preventing leakage of corporate data (should the need arise, there are exceptions to this rule, discussed in *Chapter 9, End-user Experience*).

Policy settings, such as the frequency at which logs are sent from SafeGuard PortProtector Clients to the Management Server, the wording of end-user messages and more are also defined in the policy.

You can apply a policy to any of the organizational units that are defined in your Active Directory or Novell eDirectory.

SafeGuard PortProtector takes a positive security approach, meaning all devices are blocked unless you define a policy allowing their access.

In the sections that follow we describe how to define a policy.

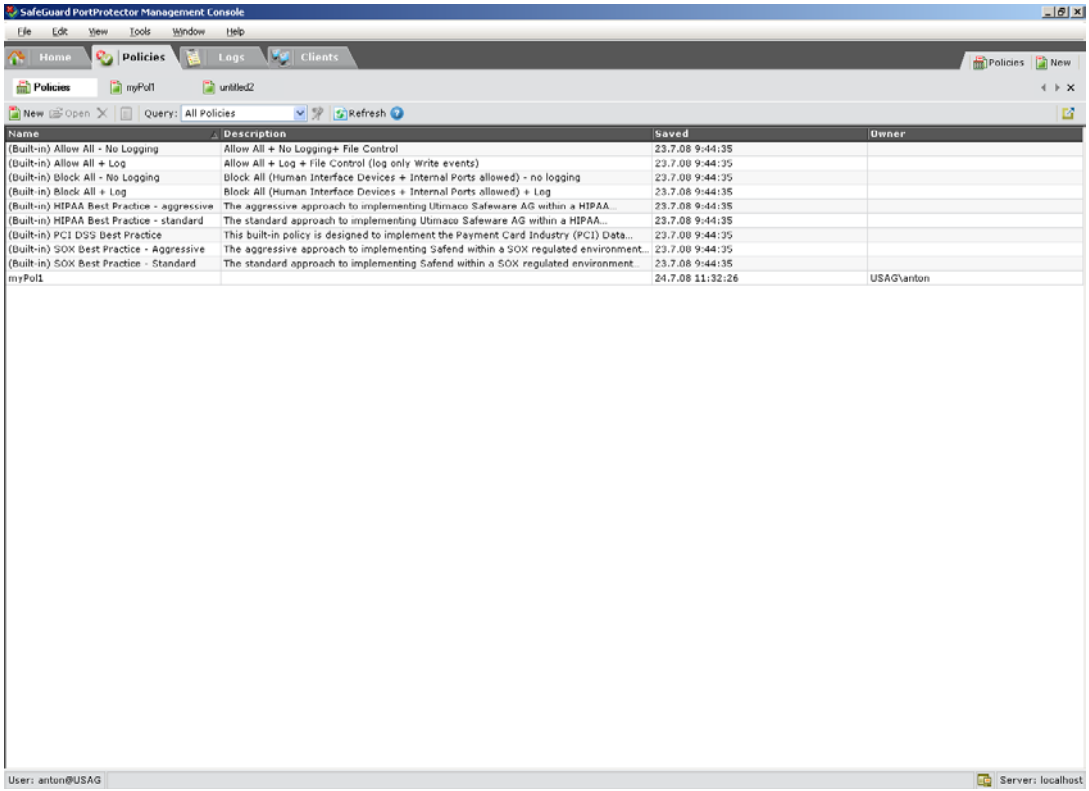
Policies start protecting the endpoints in your organization after they have been distributed to the computers in your organization, as described in *Chapter 4, Distributing Policies.*

Before we go into policy definition, we will take a quick tour of the Policies World and discuss policy management.

3.2 Quick Tour of the Policies World

To access the Policies world:

Click the **Policies** tab. The Policies window opens:


SafeGuard PortProtector Management Console
File Edit View Tools Window Help
Home Policies Logs Clients
Policies New
Policies myPol1 untitled2
New Open Query: All Policies Refresh
Name Description Saved Owner
(Built-in) Allow All - No Logging Allow All + No Logging+ File Control 23.7.08 9:44:35
(Built-in) Allow All + Log Allow All + Log + File Control (log only Write events) 23.7.08 9:44:35
(Built-in) Block All - No Logging Block All (Human Interface Devices + Internal Ports allowed) - no logging 23.7.08 9:44:35
(Built-in) Block All + Log Block All (Human Interface Devices + Internal Ports allowed) + Log 23.7.08 9:44:35
(Built-in) HIPAA Best Practice - aggressive The aggressive approach to implementing Utimaco Safeware AG within a HIPAA... 23.7.08 9:44:35
(Built-in) HIPAA Best Practice - standard The standard approach to implementing Utimaco Safeware AG within a HIPAA... 23.7.08 9:44:35
(Built-in) PCI DSS Best Practice This built-in policy is designed to implement the Payment Card Industry (PCI) Data... 23.7.08 9:44:35
(Built-in) SOX Best Practice - Aggressive The aggressive approach to implementing Safend within a SOX regulated environment... 23.7.08 9:44:35
(Built-in) SOX Best Practice - Standard The standard approach to implementing Safend within a SOX regulated environment... 23.7.08 9:44:35
myPol1 24.7.08 11:32:26 USAG\anton
User: anton@USAG
Server: localhost

The Policies World window includes the sections and control buttons described in *Know* Your Way around the Application in *Chapter 2, Getting Started*. The launch buttons and some of the menu options are particular to the Policies world.

3.2.1 Launch Buttons

The launch buttons particular to the Policies World include the following:

- **Policies**

– clicking this button opens the *Policies* window from which you can manage your policies.
- **New**

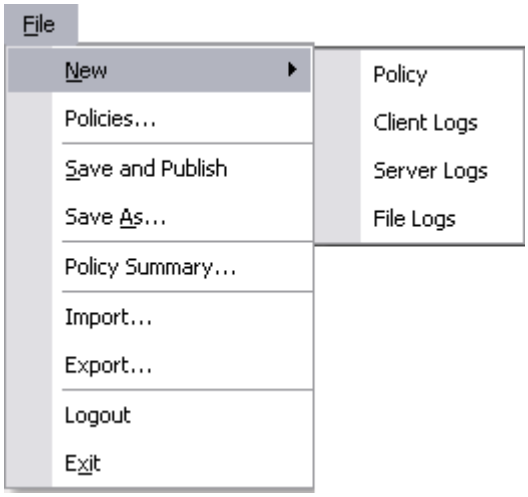
– clicking this button opens a new, untitled policy window.

3.2.2 Menus

Some of the menu options in the Policies World are particular to this world. A description of each menu and its options follows.

3.2.2.1 File Menu

The *File* menu in the Policies World enables you to open other World windows, save policies, export and import policies and more.



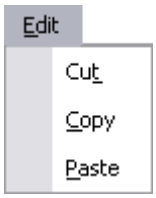
The *File* menu in the Policies World includes the following options:

Option	**Description**
New	Opens a submenu that enables you to open a new policy window, a new Clients Log window, a new Server Log window or a new File Log window.
Policies	Enables you to manage policies.
Save and Publish	Saves and publishes the policy.
Save As	Saves the policy under a new name and publishes it.
Policy Summary	Displays all policy information in a single-window, printable format.

Option	**Description**
Import	Imports an exported policy.
Export	Exports the policy to an external file.
Logout	Logs the current user out of the Management Console.
Exit	Logs out the current user and closes SafeGuard PortProtector Management Console

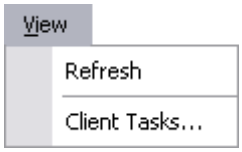
3.2.2.2 Edit Menu

The *Edit* menu provides **Cut**, **Copy** and **Paste** options for the **Add Device, Add Storage Device** or **Add WiFi Network** option described in *Approving Devices and WiFi Connections*. In other cases it is disabled.



3.2.2.3 View Menu

The *View* menu enables you to refresh the Policies window which displays a list of your policies and to view the progress of Client tasks.



The *View* menu includes the following options:

Option	Description
Refresh	Updates the list of policies to provide you with an up to date view.
Client Tasks	Displays the progress of Client tasks (for details see *Tracking Client Task Progress* in *Chapter 6, Managing Clients*).

3.2.2.4 Tools Menu

The *Tools* menu which is common to all Worlds is described in *Tools Menu* in *Chapter 2, Getting Started*.

3.2.2.5 Window Menu

The *Window* menu which is common to all Worlds is described in *Window* Menu in Chapter 2, Getting Started.

3.2.2.6 Help Menu

The *Help* menu which is common to all Worlds is described in Help Menu in *Chapter 2, Getting Started*.

3.2.3 Toolbar

The Policies world toolbar provides quick access to some commonly used functions. It appears below the menu bar, and includes the following buttons:

The following is a brief description of each toolbar button:

Button	Description
New	Click this button to open a new policy.
Open	Click this button to open the selected policy.
Delete	Deletes the selected policy.

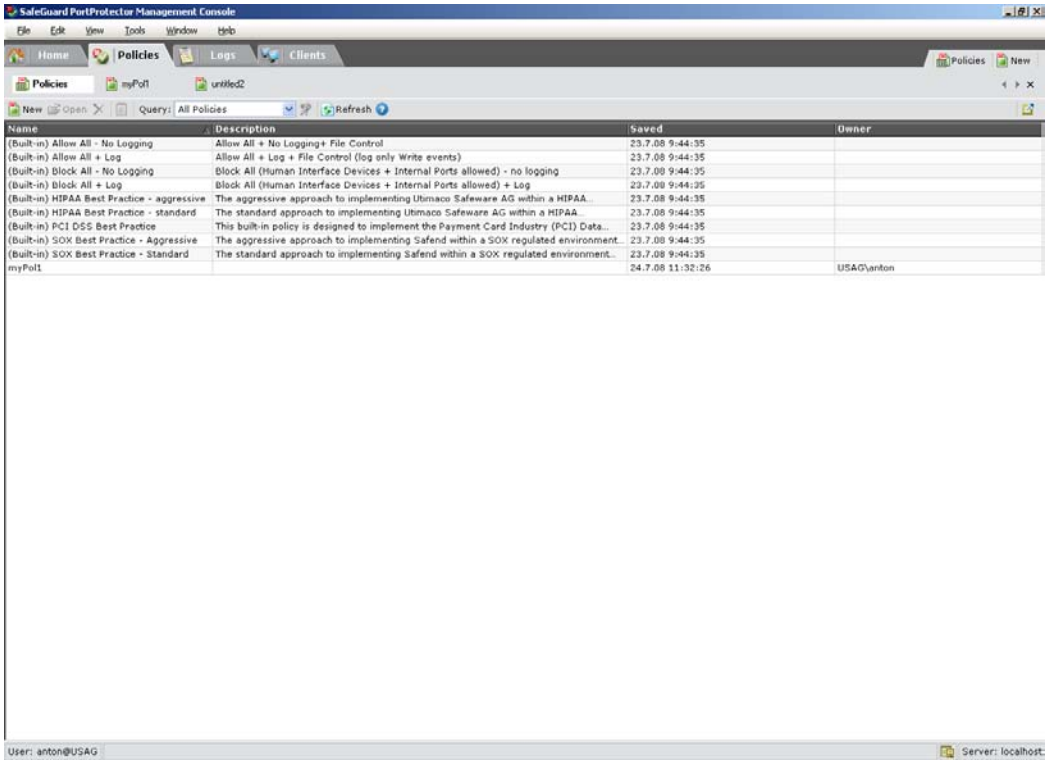
Button	Description
View Summary	Displays all policy definitions in a single-window, printable format.
Refresh	Updates the list of policies to provide you with an up to date view.
Help	Displays the context sensitive help of the active window and enables access to other help topics.

Note:

This toolbar appears in the *Policies* window which enables you to manage policies. In the Policy window, where you define policy properties, a different toolbar is available, as described in *Step 4: Define Port Control*.

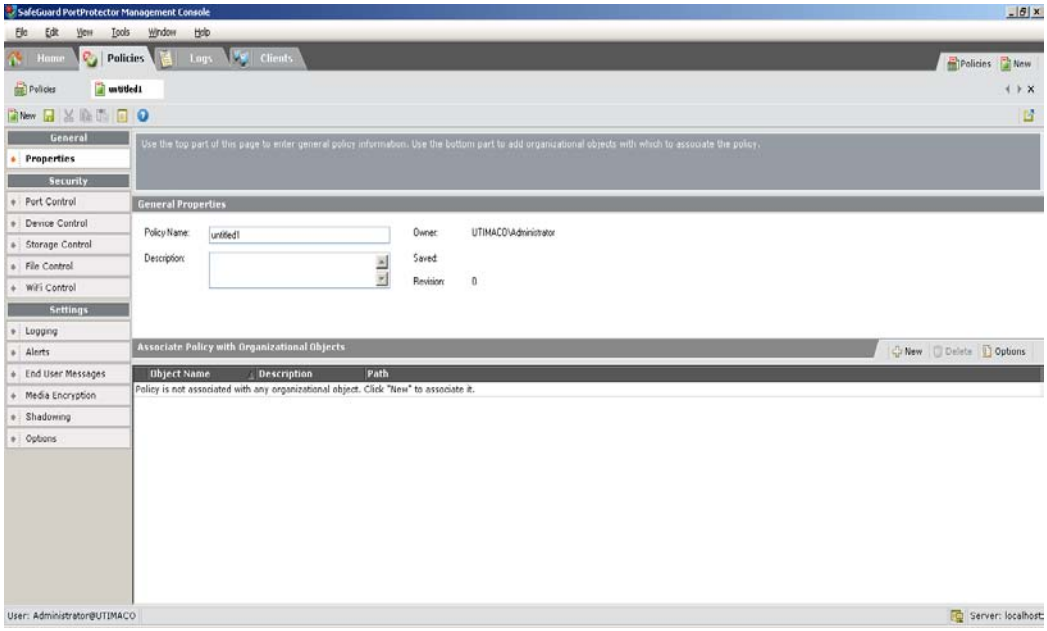
3.2.4 Workspace

The default window that opens in the workspace is the *Policies* (policy management) window:


SafeGuard PortProtector Management Console
File Edit View Tools Window Help
Home Policies Logs Clients
Policies myPol1 untitled2
New Open Query: All Policies Refresh
Name Description Saved Owner
(Built-in) Allow All - No Logging Allow All + No Logging+ File Control 23.7.08 9:44:35
(Built-in) Allow All + Log Allow All + Log + File Control (log only Write events) 23.7.08 9:44:35
(Built-in) Block All - No Logging Block All (Human Interface Devices + Internal Ports allowed) - no logging 23.7.08 9:44:35
(Built-in) Block All + Log Block All (Human Interface Devices + Internal Ports allowed) + Log 23.7.08 9:44:35
(Built-in) HIPAA Best Practice - aggressive The aggressive approach to implementing Utimaco Safeware AG within a HIPAA... 23.7.08 9:44:35
(Built-in) HIPAA Best Practice - standard The standard approach to implementing Utimaco Safeware AG within a HIPAA... 23.7.08 9:44:35
(Built-in) PCI DSS Best Practice This built-in policy is designed to implement the Payment Card Industry (PCI) Data... 23.7.08 9:44:35
(Built-in) SOX Best Practice - Aggressive The aggressive approach to implementing Safend within a SOX regulated environment... 23.7.08 9:44:35
(Built-in) SOX Best Practice - Standard The standard approach to implementing Safend within a SOX regulated environment... 23.7.08 9:44:35
myPol1 24.7.08 11:32:26 USAG\anton
User: anton@USAG
Server: localhost:

This window may be closed or opened at any time.

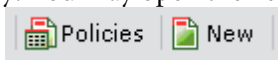
When you open a policy (whether new or existing), the following window appears:



The left hand side of the window includes the following sections:

- **General:** this section is where you enter the policy's name and description, as well as associating the policy to organizational objects. Refer to *Distributing SafeGuard PortProtector Policies Directly from the* in *Chapter 4, Distributing Policies* for an explanation of this section.
- **Security:** this section contains definitions of the policy's security settings (port control, device control, storage control, file control and WiFi control). These definitions are explained in this chapter.
- **Settings:** this section contains definitions of the policy's additional settings (loggings, alerts, end-user messages, shadowing, encryption and policy options). These definitions are explained in this chapter.

The right hand side, main part of the workspace displays various types of content, depending on the option you selected in the **General**, **Security** or **Settings** section in the left hand side of the window.

When all windows are closed, the workspace is empty. You may open the *Policies* window or a specific policy by clicking one of the launch buttons 

on the top right-hand side of the window.

Refer to *Managing Policies* to learn about policy management.

Refer to *Step 3: Create a Policy* to learn about defining policies.

3.3 Defining SafeGuard PortProtector Policies - Workflow

The following is an overview of the workflow for defining a new policy. A reference is provided from each of these steps to a sub-section that describes it in detail.

This workflow suggests a simple and straightforward order for performing these steps, from which you can deviate, if you prefer.

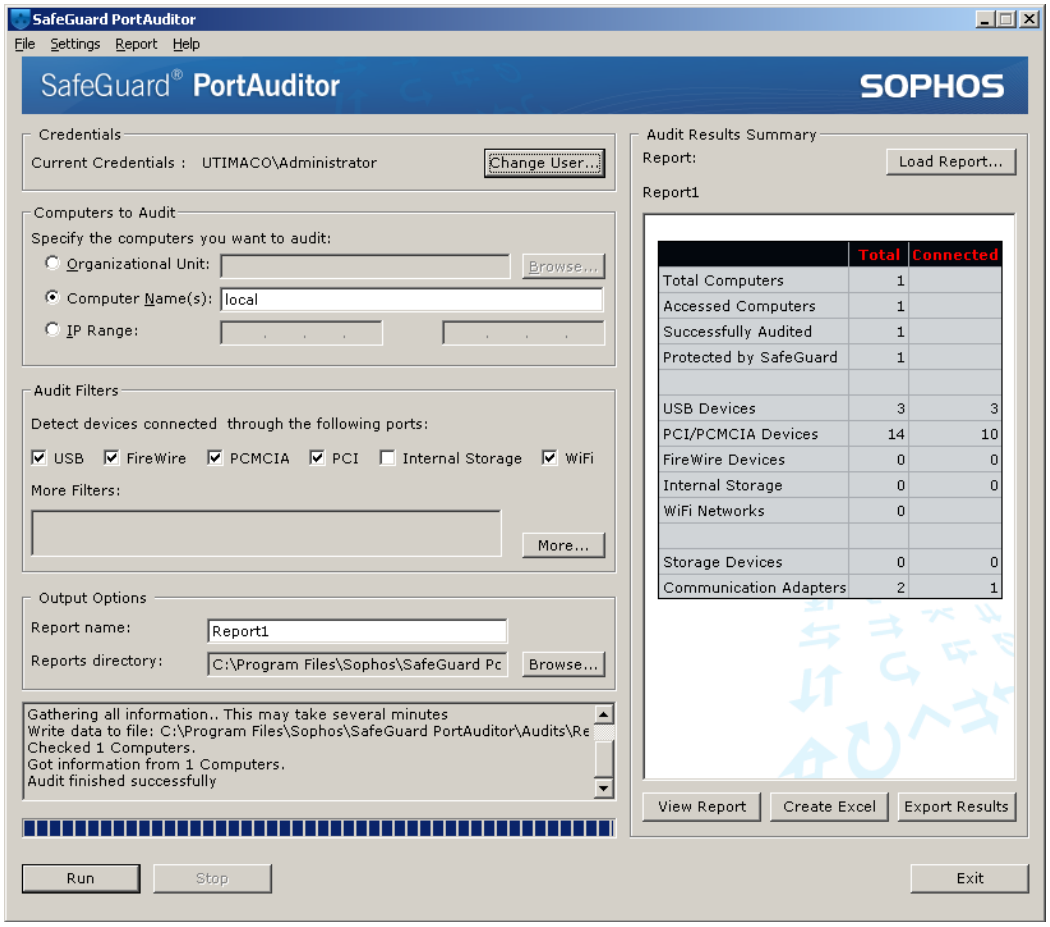
- ***Step 1: Scan Computer and Detect Port/Device/Wifi Usage***: use SafeGuard PortAuditor to scan the computers in your network in order to detect the devices and WiFi networks that are currently connected and those that were previously connected (specified in their computer's registry), as described in the SafeGuard PortAuditor User Guide. You will use this information when defining a policy in order to easily specify which ports and devices are allowed, blocked, restricted or Read Only.
- ***Step 2: Plan Your Policy*** describes the information that you should gather in order to properly plan the best endpoint protection policy for your organization.
- ***Step 3: Create a Policy*** describes how to create a new policy. You can create as many policies as needed, one for your entire organization or a different one for each group of computers or users.
- ***Step 4: Define Port Control*** describes how to define the port control aspect of your policy, meaning which ports are allowed, which are blocked and which are restricted to be used only by certain devices. Port Control also enables you to specify log and alert options for port initialization and/or activity. In addition, this section described how to prevent hybrid network bridging.
- ***Step 5: Define Device Control*** describes how to define more specifically which devices are allowed to connect through the restricted ports on your endpoints. Device Control also enables you to specify log and alert options for device activity.***Step*** 6: Define Storage Control describes how to define more specifically which storage devices are allowed to connect to your endpoints and which should only connect in Read Only or encrypted mode. Storage Control also enables you to specify log and alert options for activity on a storage device type, device model or distinct storage device.
- ***Step 7: Define File Control*** describes how to control files written to or read from storage devices, shadow, track or inspect their content, according to their type. It also enables you to specify log and alert options for written and read files according to their type.
- ***Step 8: Define WiFi Control*** describes how to define which WiFi connections are approved. It also describes how to specify log and alert options for WiFi activity
- ***Step 9: Define Global Policy Settings*** describes how to define defaults for the logging, end-user message and options settings described in steps 10-16 below.
- ***Step 10: Define Logging*** describes how to define logging settings for the current policy, such as the frequency at which log entries are sent to the SafeGuard PortProtector log repository from a protected endpoint.
- ***Step 11: Define Alerts*** describes how to select destinations for alerts originating from an endpoint protected by this policy
- ***Step 12: Define End User Messages*** describes how to define the messages that are displayed to the end-user by the SafeGuard PortProtector Client on each computer.

- ***Step 13: Define Media Encryption*** describes how to define encryption settings when the policy requires encryption, including endpoint behavior when an attempt is made to access a non-encrypted device and authorization of access to an encrypted device when not connected to the organizational network.
- ***Step 14: Define File Shadow Settings*** describes how to enable you to define SafeGuard PortProtector settings for tracking and collecting copies of files that have been moved to/from external storage devices.
- ***Step 15: Define Options*** enables you to define various behavioral aspects of the SafeGuard PortProtector Client on the endpoints.
- ***Step 16: Defining Policy Permissions*** describes how to define to which administrators the policy will be visible if you are using the SafeGuard PortProtector Domain Partition-based management ability.
- ***Step 16: Save and Publish the Policy*** describes the options for saving the policy in the policy database and publishing it so that it can be associated to the relevant Clients.

Once SafeGuard PortProtector Policies are distributed and applied to SafeGuard PortProtector Clients, they implement your protection policy on each computer. You may refer to *Chapter 4, Distributing Policies* for a description of how to distribute SafeGuard PortProtector policies to the endpoints of your organization.

3.3.1 Step 1: Scan Computers and Detect Port/Device/Wifi Usage

Although not an integral part of SafeGuard PortProtector, SafeGuard PortAuditor is a tool that goes hand in hand with SafeGuard PortProtector and completes it by providing you with a full view of what ports, devices and networks are (or were previously) in use by your organization's users. You use the output of a SafeGuard PortAuditor scan to select the devices and networks whose usage you want to approve.



You may launch SafeGuard PortAuditor from within SafeGuard PortProtector, as described in *Auditing Devices in Chapter 6, Managing Clients.* More detail is provided in the *SafeGuard PortAuditor User Guide*.

3.3.2 Step 2: Plan Your Policy

Before you start defining your policy, you should take the time to plan the policy best suited to your organization. The best SafeGuard PortProtector Policy for your organization is one that meets its security needs while still fulfilling the requirements of the people who need access through the ports your organization's computers.

The first thing to plan for is the types of OU (Organizational Units) groups to which the policies will apply.

3.3.2.1 User and Computer Policies

By default, SafeGuard PortProtector uses User Group and Computer Group definitions that are controlled by Active Directory (for details about Novell eDirectory support refer to *Appendix A – Novell eDirectory Synchronization*). Each option has its own benefits, as described below.

- **Per User Groups:** Defining your policies per user groups enables you to be specific regarding the permissions for each user.

  Policies that apply to users override policies that apply to computers.
  If you decide to manage your organization by assigning policies to user groups, we recommend that you still define one or more general policies for computers. This enables the protection of each computer port even when no user is logged in.
  Using the combination of user policies and computer policies means that, for example, you can block USB storage devices on all the Customer Service department's computers, but you can allow the manager of the department a more permissive policy according to his/her username and password, regardless of the computer into which he/she is logged.
- **Per Computer Groups:** Defining your policies by computers enables the protection of the endpoints of your organization's computers regardless of the user who is logged in.

SafeGuard PortProtector enforces policies as follows: it first applies a user policy, if one exists for the user that is currently logged in. If not, SafeGuard PortProtector looks for a policy that applies to the computer, and uses it, if found. This means that when no user is logged in, the computer-bound policy is used. It is therefore advised to distribute user-based policies, so that a user is given the same policy regardless of the computer into which he or she is logged, and to set computer based policies that are more restrictive. These computer-based policies should still grant access to such devices as a mouse and keyboard, to be used when no user, or a user outside of the domain, is logged in.

The initial configuration of the SafeGuard PortProtector Client allows all port and device activity, meaning that nothing is blocked. A permissive configuration is necessary so that all port activity is not automatically blocked immediately following the installation of the SafeGuard PortProtector Client.

This means that until you actually define and distribute policies to your endpoints (per user or per computer), the machine that was just installed with SafeGuard PortProtector Client will continue to operate as before (no blocking of ports and devices).

Note: If a policy on the endpoint is tampered with, SafeGuard PortProtector immediately invokes a panic mode that blocks all access to ports and devices.

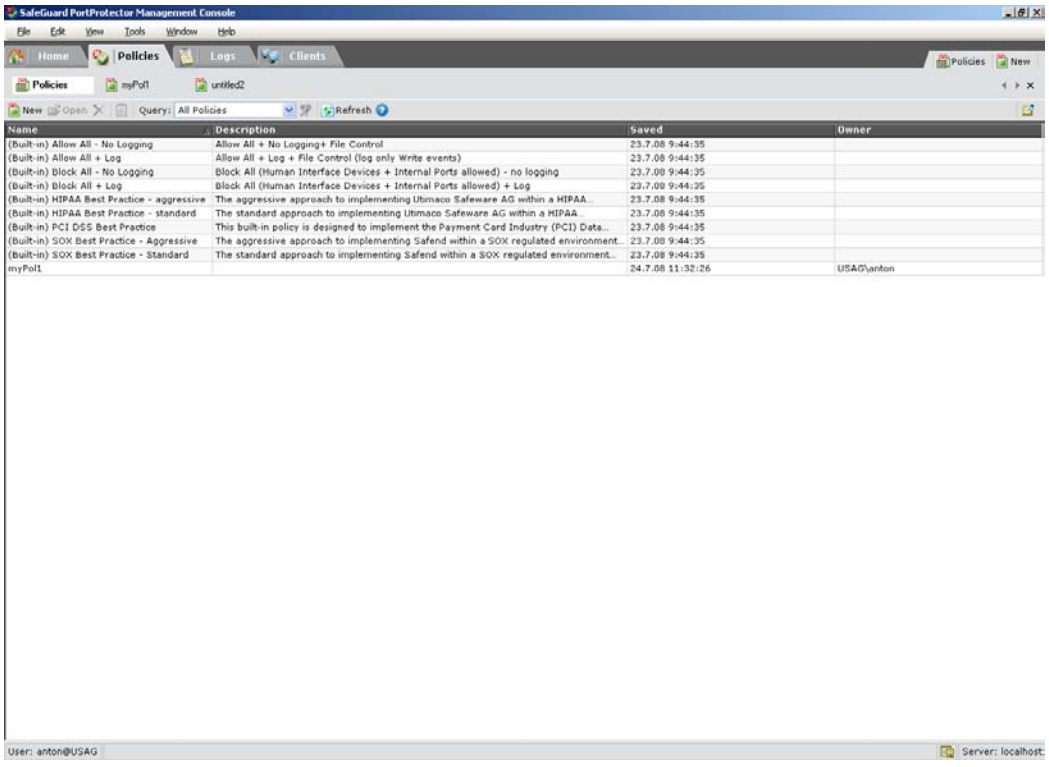
3.3.3 Step 3: Create a Policy

This section describes how to create a new policy in the Policies World. You can start from the default settings or from a template (described in *Policy Template* in *Chapter 7, Administration*) or use an existing policy as your starting point.

SafeGuard PortProtector comes with several built-in policies which you may use to start you off, if you wish. These include:

- (**Built-in**) **Allow All – No Logging:** all devices and files are allowed, no logging is performed.
- (**Built-in**) **Allow All + Log:** all devices and files are allowed, logging of device activity is performed, logging of written files is performed.
- (**Built-in**) **Block All – No Logging:** all devices except human interface devices (HIDs) are blocked, no logging is performed.
- (**Built-in**) **Block All + Log**: all devices except human interface devices (HIDs) are blocked, logging of device activity is performed, logging of written files is performed.

Click on the *Policies* tab to open the Policies World.


SafeGuard PortProtector Management Console
File Edit View Tools Window Help
Home Policies Logs Clients
Policies myPol1 untitled2
New Open Query: All Policies Refresh
Name Description Saved Owner
(Built-in) Allow All - No Logging Allow All + No Logging+ File Control 23.7.08 9:44:35
(Built-in) Allow All + Log Allow All + Log + File Control (log only Write events) 23.7.08 9:44:35
(Built-in) Block All - No Logging Block All (Human Interface Devices + Internal Ports allowed) - no logging 23.7.08 9:44:35
(Built-in) Block All + Log Block All (Human Interface Devices + Internal Ports allowed) + Log 23.7.08 9:44:35
(Built-in) HIPAA Best Practice - aggressive The aggressive approach to implementing Utimaco Safeware AG within a HIPAA... 23.7.08 9:44:35
(Built-in) HIPAA Best Practice - standard The standard approach to implementing Utimaco Safeware AG within a HIPAA... 23.7.08 9:44:35
(Built-in) PCI DSS Best Practice This built-in policy is designed to implement the Payment Card Industry (PCI) Data... 23.7.08 9:44:35
(Built-in) SOX Best Practice - Aggressive The aggressive approach to implementing Safend within a SOX regulated environment... 23.7.08 9:44:35
(Built-in) SOX Best Practice - Standard The standard approach to implementing Safend within a SOX regulated environment... 23.7.08 9:44:35
myPol1 24.7.08 11:32:26 USAG\anton
User: anton@USAG
Server: localhost

There are several approaches for starting off a new policy:

- **From the default values or a template:** When you open a new policy, the policy window opens with the system default policy definitions.
- **Based on an existing policy:** If you have already defined policies through the Management Server Console, you can use any of these definitions as a basis for a new policy, either by duplicating and existing policy or by saving it under a new name.
- **Based on a policy template:** You may also define a policy template which will serve as a basis for new policy definitions instead of the default values (refer to *Policy Template* in *Chapter 7, Administration*).

3.3.3.1 Creating a New Policy

This section explains how to create a new policy from scratch.

To create a new policy:

In the Policies World, from the tab at the top right, click **New** ( )

OR

From the toolbar, click **New**

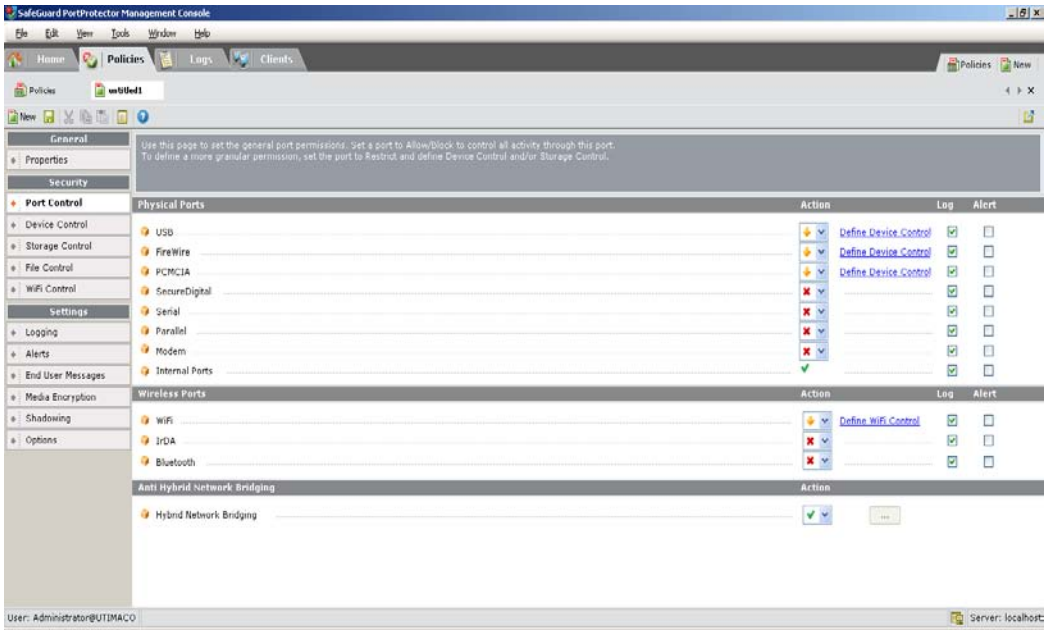
OR

In the Window bar, right-click a policy and select **New Policy**

OR

From the *File* menu, select **New.**

The *Properties* tab opens, displaying a new, untitled policy:



3.3.3.1.1 Policy Properties

This window enables you to enter the policy's name and a description. A new policy contains the default values, or with the policy template values if you have defined such a template (refer to *Policy Template* in *Chapter 7, Administration*).

3.3.3.2 Creating a New Policy from an Existing Policy

This section explains how to create a new policy from an existing policy.

To create a new policy from an existing policy:

1 Open the existing policy as explained in *Managing Policies* and modify it as required.

2 From the *File* menu, select **Save As** and save under a new name.

Alternatively, you can duplicate an existing policy and save it under a new name, as explained in *Duplicating a Window* in *Chapter 2, Getting Started*.

The following steps explain how to define and save your policy.

3.3.4 Step 4: Define Port Control

This step includes setting port permissions as well as hybrid network bridging permissions.

Port Permissions

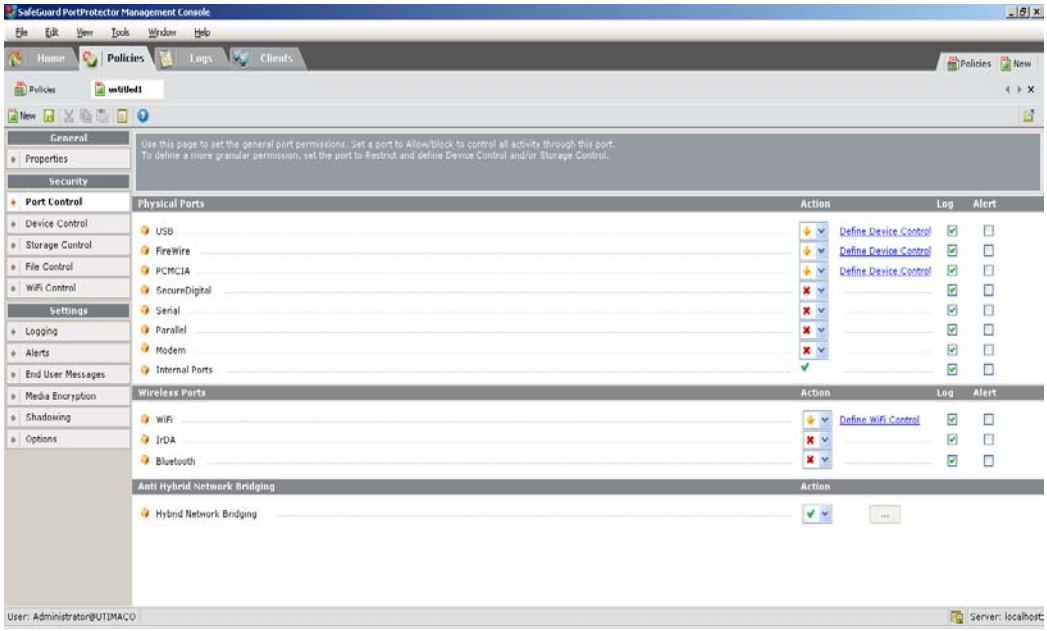
SafeGuard PortProtector enables positive security by blocking access to all ports in all computers to which a policy is distributed unless that policy specifies that access to that port is allowed, as follows. For each port (USB, FireWire, PCMCIA, Secure Digital, Serial, Parallel, Modem, WiFi, IrDA or Bluetooth), you can specify the following:

- **Allow:** This option specifies that the port can be used for any purpose, without any restrictions on this communication channel.
- **Block:** This option means that no access can be performed through this port. The port is unavailable as if its wires were cut. When a port is blocked, you can specify that port initialization attempts be logged or that that they trigger alerts.

Restrict: For USB, FireWire, PCMCIA and WiFi ports you also have the option to specify that access to ports of this type is Restricted. A **Restricted** setting enables you to define more specifically (meaning with higher granularity) which devices or connections are allowed to access the port. For example, you can specify that only USB devices of a specific model or even specific USB devices (meaning distinct devices with a unique serial number) are allowed access. For physical ports, this is done using the **Device Control** option described in *Step 5: Define Device Control* and the **Storage Control** option described in*Step 6: Define Storage Control* **Note:** *The Device Contr*ol and *W*iFi Control aspects of a policy only apply to **ports that a**re restricted. The Storage Control aspect of a policy applies both to restricted and allowed ports.

To define Port Control:

1 Display the *Port Control* window by selecting the **Port Control** button in the *Security* menu on the left, as shown below:



- The toolbar that appears when viewing or modifying a policy is different than the previously described toolbar, which appears when viewing the initial Policies window:

The following is a brief description of each toolbar button:

Button	Description
New	Click this button to open a new policy.
Save and Publish	Click this button to save and publish the policy.
Cut	Click this button to cut a group from the white list (enabled in Device Control and Storage Control tabs when white list groups have been added).
Copy	Click this button to copy a group from in the white list (enabled in Device Control and Storage Control tabs when white list groups have been added).

Button	Description
Paste	Click this button to paste a group in the white list (enabled in Device Control and Storage Control tabs when a white list group has been cut or copied).
Policy Summary	Click this button to display all policy definitions in a single-window, printable HTML format.
Help	Click this button to display the context sensitive help of the active window and to enable access to other help topics.

- The *Action* menu enable you to specify whether a port is Allowed or Blocked. USB, FireWire, PCMCIA and WiFi ports can also be Restricted.
- The *Log* checkboxes enable you to specify whether port initialization and/or port activity are logged and whether alerts are triggered for port events.
- The *Alert* checkboxes enable you to specify whether alerts should be triggered for port events.

2 For each port, specify whether its action type is Allow ( ), Block ( ) or Restrict ( ) by selecting the appropriate option in the drop down field in the Action menu. The meaning of each of these options is described at the beginning of this section.

3 If you selected Restrict in the previous step for the USB, FIREWIRE, PCMCIA ports, the Define Device Control link appears to the right of the drop-down field. The Device Control window can be accessed through this link or by selecting the Device Control button in the Security menu. Use one of these options to define the device models or distinct devices that are allowed access through this port. More detail is provided in Step 5: Define Device Control.

4 If you selected Restrict in the previous step for the WiFi port, the Define WiFi Control link appears to the right of the drop-down field. The WiFi Control window can be accessed through this link or by selecting the WiFi Control button in the Security menu. Use one of these options to define the allowed WiFi connections. More detail is provided in *Step 5: Define Device Control*.

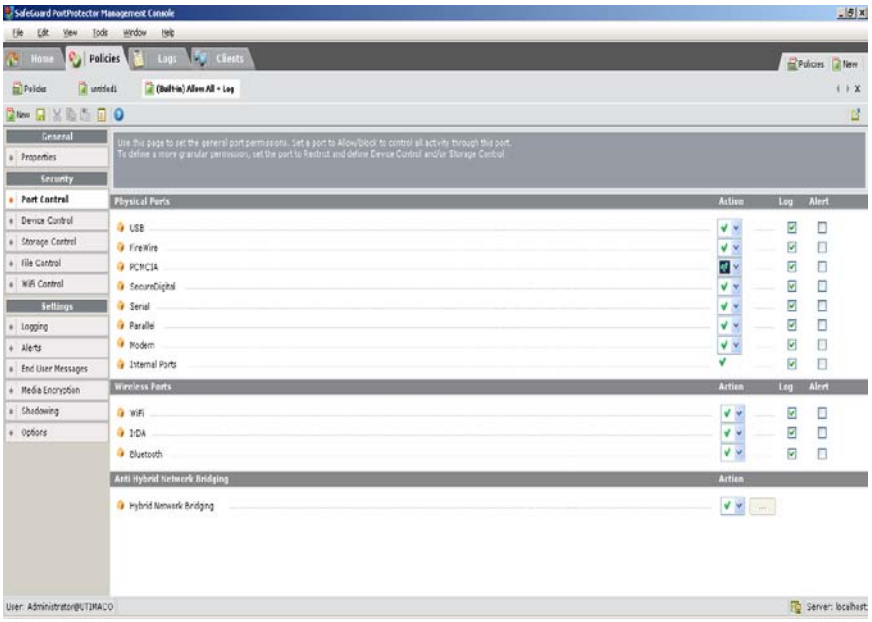
5 For each port, in the **Log** checkbox, specify whether port initialization should be logged for this port. When this checkbox is checked, an event is recorded in the SafeGuard PortProtector log each time a port is initialized. This is true for Internal Ports as well.

6 For each port Specify whether port initialization triggers an alert (in addition to being logged) by checking the **Alert** checkbox for this port (an alert must always be accompanied by a log record. Therefore, when the **Alert** checkbox is checked, the **Log** checkbox is automatically checked).

Tip:

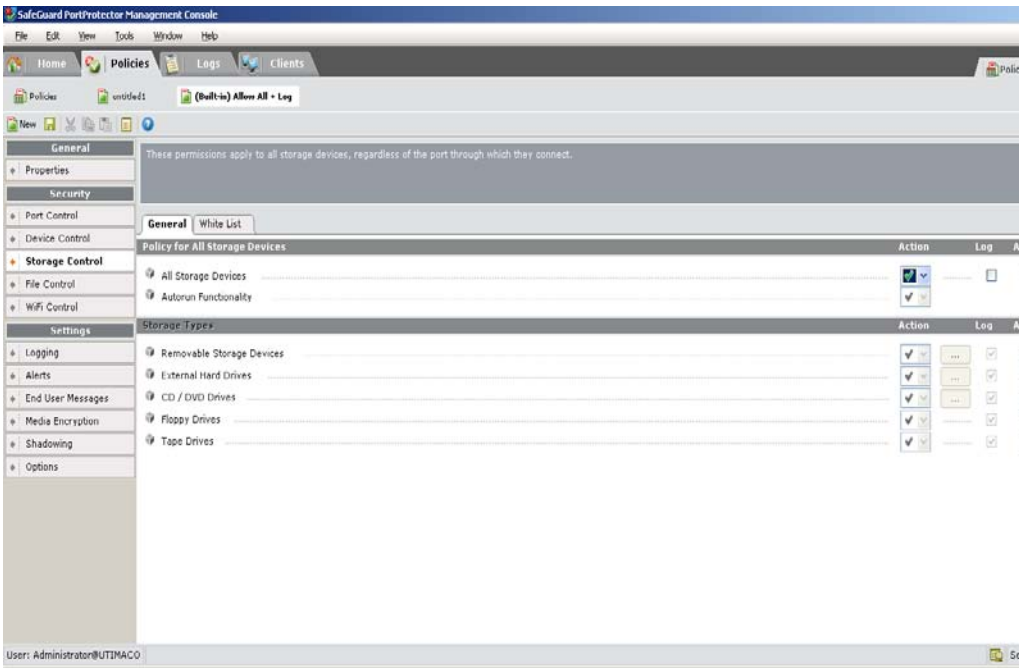
Initially, after you install SafeGuard PortProtector, you may prefer to use one of the built-in policies (see *Step 3: Create a Policy*). Alternatively, you may choose to create and distribute a very permissive policy that allows access to all ports (not blocked or restricted) and simply logs activities.

In this case you will set the ports to **Allow**, and will check the **Log** checkbox for each port. The **Port Control** options of such a policy may appear as follows:



You will also need to **Allow** "All Storage Devices" as follows:

During the initial implementation of SafeGuard PortProtector, you may want to run this permissive policy for a few days and monitor the port activity of your organization. This may help you determine the most suitable policy to define and distribute for your organization.



Note: SafeGuard PortProtector also monitors internal computer ports. Internal ports include storage busses such as IDE, SCSI, ATA and S-ATA, which are used to connect internal hard disk drives as well as PCI and PCI-X which cater to devices such as modems and network cards.
In the case of Internal Ports, the *Action* is always Allow, as these ports can be monitored but not controlled. Changes detected with regards to these ports can be logged and/or set to issue an alert. This is useful in scenarios such as the following: sophisticated malicious users may connect an additional hard disk drive to their internal IDE bus in order to extract corporate information to this device without leaving any trace. With this feature, administrators can get immediate alerts on any connection or disconnection of devices to the internal ports of protected endpoints.

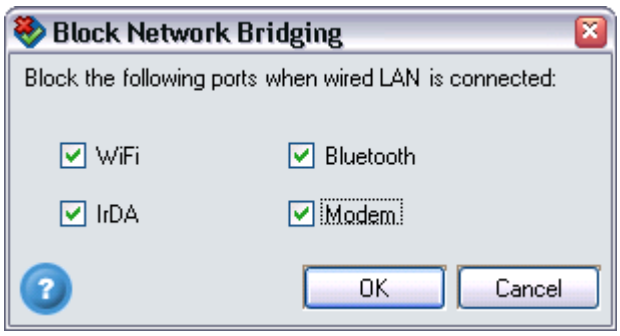
Hybrid Network Bridging Permissions

SafeGuard PortProtector allows administrators to control and prevent simultaneous use of various networking protocols that can lead to inadvertent or intentional hybrid network bridging (such as WiFi bridging and 3G card bridging). Configuring SafeGuard PortProtector Clients to block access to WiFi, Bluetooth, Modems or IrDA links while the main wired TCP/IP network interface is connected to a network enables users to employ certain networking protocols only when they are disconnected from the network - avoiding the creation and potential abuse of a hybrid network bridge.

Hybrid Network Bridging permissions are set in the *Block Network Bridging* window.

To open the Block network Bridging window:

Click the button. The Block Network Bridging window opens:



You can now set anti hybrid network bridging permissions as explained in *Blocking hybrid Network Bridging*.

3.3.4.1 Blocking hybrid Network Bridging

The *Block Network Bridging* window is where you define which wireless ports should be blocked when the endpoint is connected to the wired LAN.

To block hybrid network bridging:

Leave checkboxes checked for those ports you wish to block while connected to the wired LAN. Uncheck the checkboxes for the ports you wish to allow.

3.3.5 Step 5: Define Device Control

In the *Port Control* window, for USB, FIREWIRE and PCMCIA ports you can specify that access to ports of these types is restricted (this is true for WiFi ports, too, which is discussed in *Step 8: Define WiFi Control*). Selecting **Restrict** enables you to define more specifically, using the **Device Control** window, which devices are allowed to access these ports.

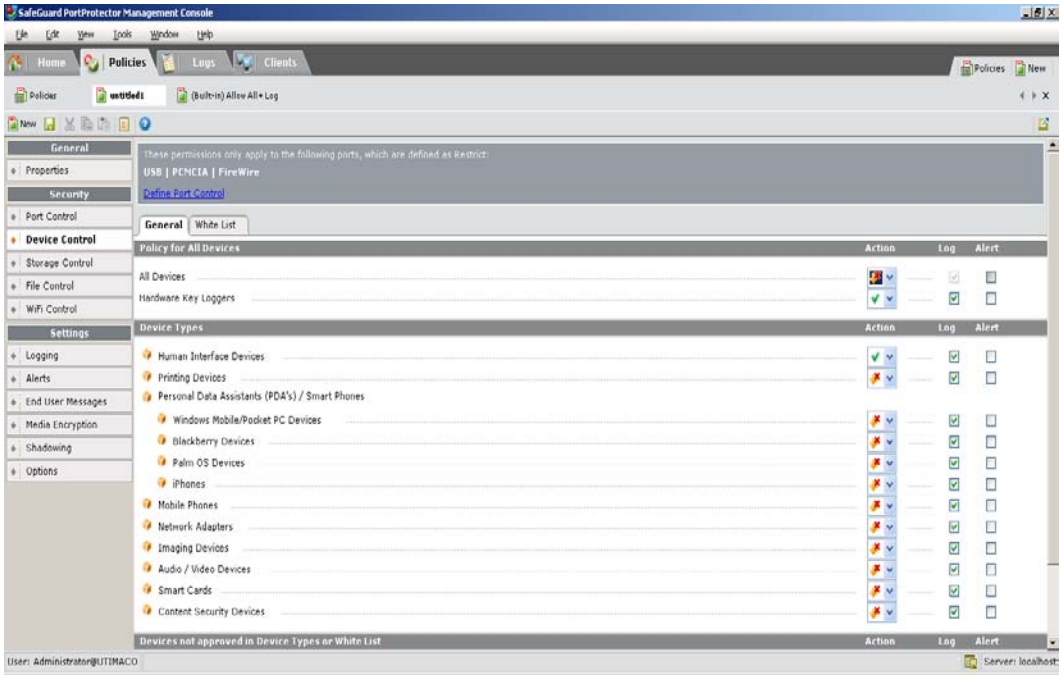
To display the *Device Control* window:

1 In the *Security* menu on the left, click the **Device Control** button

OR

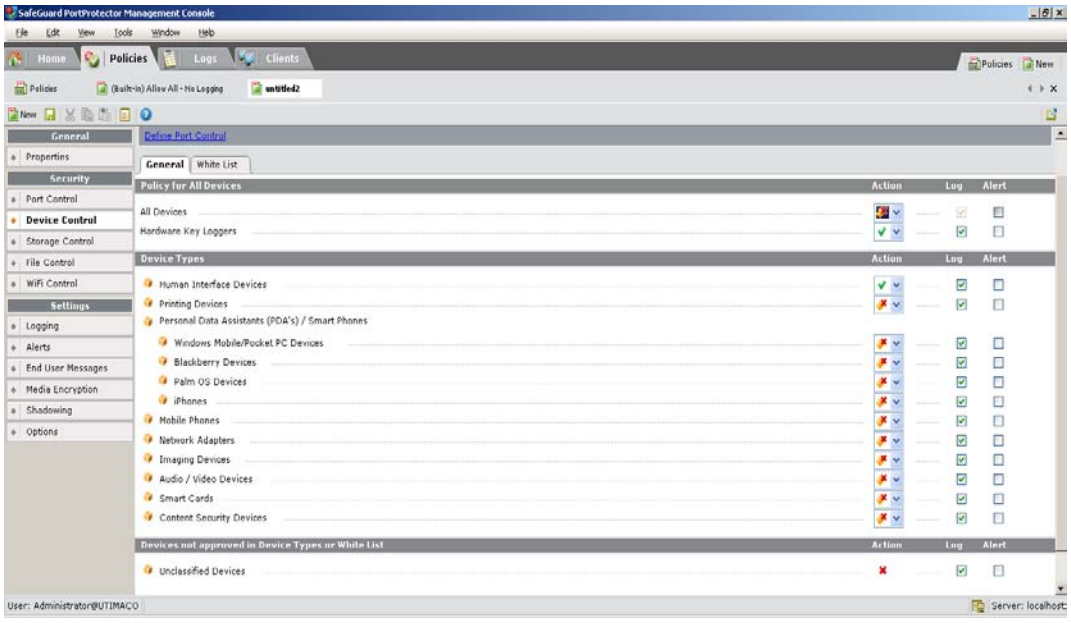
In the *Port Control* window, click the **Define Device Control** link to the right of the USB, FireWire or PCMCIA option.

2 The following window opens:



The *Device Control* window includes two tabs: the *General* tab, shown in the figure above, which you use to specify which device types are allowed access, and the *White List* tab, which you use to specify which device models or distinct devices are allowed access. If a device is not defined as allowed in one of the ways described below, then it is blocked. The Device Control aspect of a policy applies to **all** the ports that are Restricted.
In addition, *Device Control* enables you to specify activity Log and Alert options down to the distinct device group level. This means that you may choose to log activities for mobile phones in general, for example, but not to log activity for a specific group of allowed mobile phones.

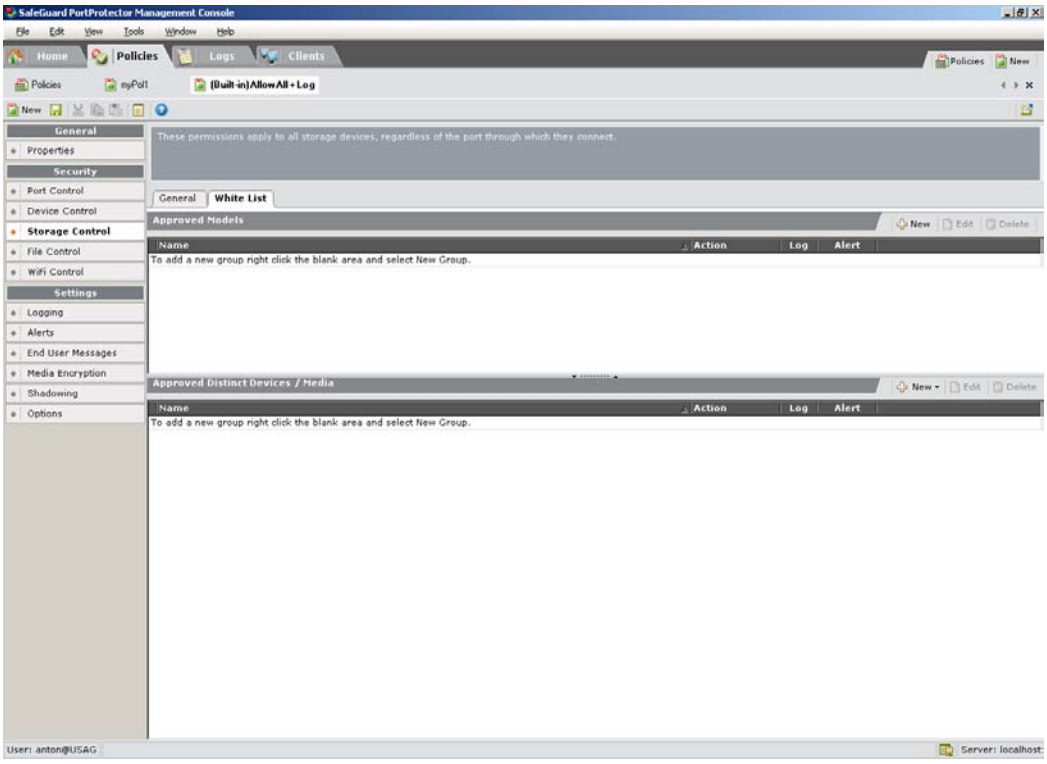
3.3.5.1 Device Control - General Tab



- **Policy for All Devices** (top area): in this area you can **Allow**, **Restrict** or **Block** access to all device types. If you select **Allow** or **Block** for **All Devices**, the rest of the window is disabled. This is where you set log and alert definitions for device activity if USB, FireWire or PCMCIA ports are allowed or blocked.
  You can also **Allow** or **Block** - and define log and alert settings for - hardware key loggers (hardware key loggers are discussed in *Protection against Hardware Key Loggers* in *Chapter 1, Introducing SafeGuard PortProtector*).
- **Devices Types** (middle area): if you have selected the **Restrict** option for *All Devices* as described in the previous paragraph, this option enables you to allow or restrict access to a device according to its type. For example: Printing Devices, Network Adapters or Imaging Devices. The device types available for selection are built into SafeGuard PortProtector. If you would like to allow a device that is not of one of the types listed here, add it to your list of approved devices – the **White List** - using the **Approved Model** or the **Distinct Devices** option, described below. A list of the supported Device Types is provided in *Appendix B - Supported Device Types*.
- **Devices Not Approved in Device Types or White List** (bottom area): if you have selected the **Restrict** option for *All Devices*, this option enables you to determine whether the attempted activity of devices of unknown types (these devices are blocked, by default) should be logged and/or an alert be generated. See
- Allowing / Blocking Access to Unclassified Devices for more details.

For an explanation of how to define options in this window refer to *Defining Device Control.*

3.3.5.2 Device Control - White List Tab



Above the tab, a message appears displaying the ports which you have set to **Restrict**. If you want to change port settings, do so in the *Port Control* window (you can click Define Port Control to switch to the *Port Control* window).

The window is divided into two areas:

- **Approved Models** (top area): This option refers to the model of a specific device type, such as a specific model of HP printers, such as LaserJet 4050N.
- **Approved Distinct Devices** (bottom area): This option refers to distinct devices with a unique serial number, meaning an actual specific device. For example: the CEOs personal printer may be permitted to connect, while other printing devices are not.

You use both these areas to add approved device groups.

On the right hand side of the tab, three buttons are available:

- **New Group** ( ): use this button to add a new device group.
- **Edit Group** ( ): use this button to edit a device group.
- **Delete Group** ( ): use this button to delete a device group.

Note:

This window is disabled whenever you select the **Allow** or **Block** option in **Policy for All Devices** in the *General* tab. See *Defining Device Control*.

Important:

In cases where a device belongs to more than one group, and those groups have the same permissions, SafeGuard PortProtector will choose between the groups arbitrarily. If the groups do not have the same log and alert settings, it cannot be predicted which settings will apply.

For an explanation of how to define options in this window refer to *Defining Device Control.*

3.3.5.3 Defining Device Control

To define Device Control:

1 In the *Device Control* window, click the *General* tab if it is not the active tab.
The top part of the window lists the ports that were defined as **Restricted** in the *Port Control* window, described in *Step 4: Define Port Control.* The devices that you will allow or block in the *Device Control* window, described in this section, only apply to these ports.

2 In the *Policy for All Devices* section, specify in the *Action* drop-down menu whether All Devices are **Allowed** ( ), **Restricted** ( ) or **Blocked** ( ).

Note: Select **Allow** or **Block** when you do not want to apply granular device control at this point in time. Alternatively, use this option when you wish to override existing granular definitions but want to return to them at a later time.

3 If you select **Allow** or **Block** for *All Devices*, you can also specify whether device activity should be logged and/or whether alerts should be generated by checking the **Log** and/or **Alert** checkboxes.
If you select **Allow** or **Block** for *All Devices*, there is nothing more you need to do in the *Device Control* window and you can now skip to *Step 6: Define Storage* Control.
If you select Restrict for All Devices, set log and alert definitions for the various device types in the Device Types section as described below.

4 If you selected **Restrict** for *All Devices*, define whether Hardware Key Loggers (explained *in Protection against Hardware Key Loggers in Chapter 1, Introducing SafeGuard PortProtector*) are **Allowed** or **Blocked**. You may also define whether identification and /or blocking of a Hardware Key Logger should be logged and/or whether alerts should be generated.

Note: If the SafeGuard PortProtector Client suspects a USB Hardware Key Logger is connected to the keyboard, and Hardware Key Loggers are **Blocked**, the keyboard is blocked, too. To activate the keyboard, advise the user to connect it directly to the computer. Additionally, you may reset the SafeGuard PortProtector Client's memory so as to allow the keyboard to resume work in the present state (this is explained in *Reset Keyboards (approve keyboard hubs)* in *Chapter 9, End-user Experience*).

Note: When you block Hardware Key Loggers, both USB and PS/2 Key Loggers are blocked. When SafeGuard PortProtector Client protects against PS/2 Key Loggers, no user message is displayed. Nevertheless, the Key Logger device is rendered useless, since the information it logs is scrambled.

In addition, note that when a PS/2 Key Logger is blocked while working with a PS/2 Keyboard Video Mouse (KVM), the KVM switching between computers will not work from the keyboard. You can switch computers by pressing the KVM itself.

5 If you selected **Restrict** for *All Devices*, set permissions for each **Device Type** in the *Action* drop-down menu as follows:

- **Allow** ( ): allows all devices of this type.
- **Restrict** ( ): all devices are blocked unless they are specifically approved in the *White List* tab described in *Approving Devices and WiFi Connections*.

6 Check the **Log** checkbox if you want device activity to be logged. When this checkbox is checked, an event is logged whenever a device of this type is connected, which can be viewed in the Logs World.

7 Check the **Alert** checkbox if you want device activity to trigger an alert. Alerts can also be viewed in the Logs World.

8 Define the **Log** and/or **Alert** options for *Unclassified Devices* in the **Devices Not Approved in Device Types or White List** area at the bottom of the window. The **Action** field cannot be edited in this window. Access to unclassified devices is defined in the *Policies* tab of the *Administration* window. The settings there determine whether **Blocked** ( ) or **Allow** ( ) appears here.

9 Select the **Approved Models** and **Distinct Devices** to add to your allowed devices in the *White List* tab as described in *Approving Devices and WiFi Connections*.

3.3.6 Step 6: Define Storage Control

Storage devices may typically be the main conduits for information leakage in an organization. Therefore, all storage units are blocked by default unless you specify otherwise.

SafeGuard PortProtector enables you to control access by allowing full access, blocking or allowing Read Only access by any device that is identified as a storage device. This includes removable media such as disk-on-keys, digital cameras and so on, as well as traditional devices, such as floppy drives, CD/ DVD drives, external hard disks and tape drives. For Removable Storage Devices, it also enables you to limit access to organizationally encrypted devices only (see *SafeGuard PortProtector Removable Storage Encryption* in *Chapter 1, Introducing SafeGuard PortProtector*.

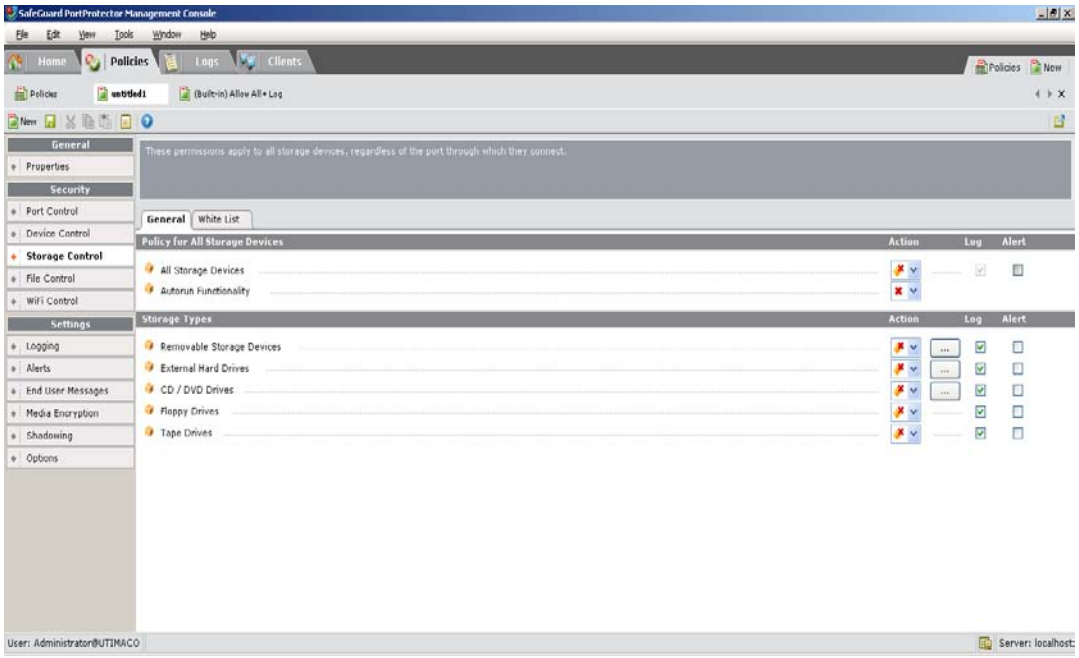
Note: The **Read Only** option is not available for tape drives.

The Storage Control aspect of a policy is enforced across all ports through which a storage device can connect. This includes **Allowed** or **Restricted** ports, as well as ports that are not protected by SafeGuard PortProtector. On a port that is **Blocked** all storage devices are blocked, since blocking a port is similar to cutting its wires.

3.3.6.1 Displaying the Storage Control Window

To display the *Storage Control* window:

Click the **Storage Control** button in the *Security* menu on the left. The following window opens:



The *Storage Control* window includes two tabs: the *General* tab, which you use to specify which storage types are allowed access, and the *White List* tab, which you use to specify which device models or distinct devices are allowed access.

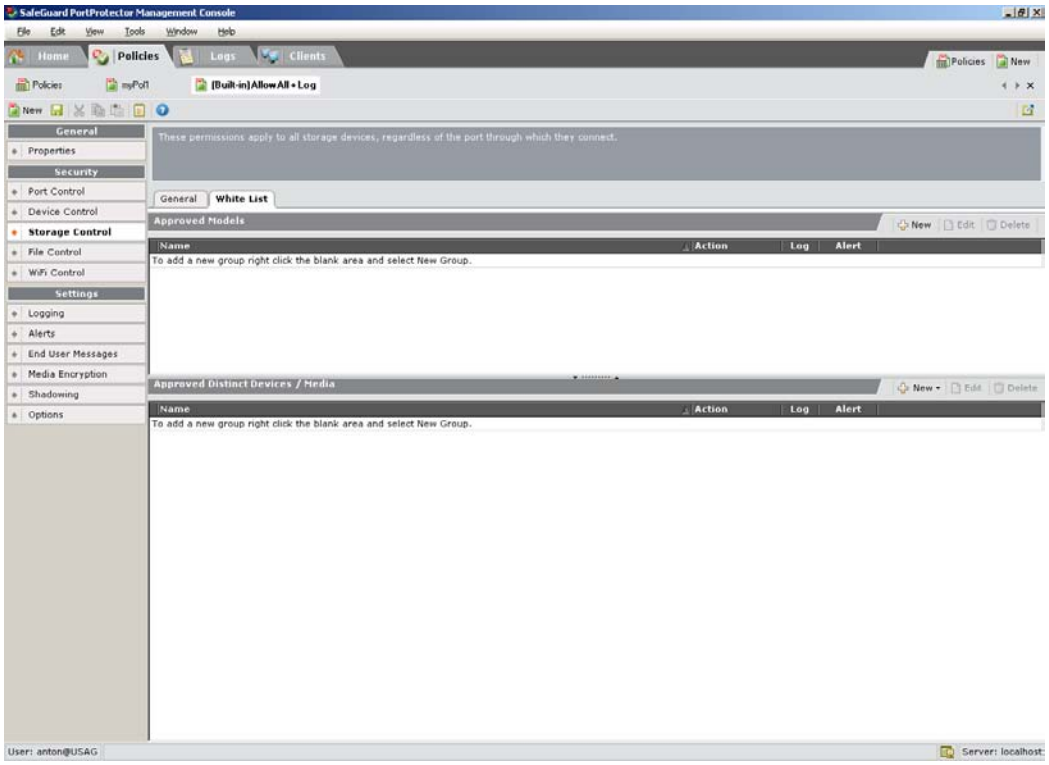
3.3.6.2 Storage Control - General Tab

- This window includes the following areas:
- **Policy for All Storage Devices** (top area): in this area you can **Allow**, **Restrict** or **Block** access to all storage devices. If you select **Allow** or **Block** for **All Storage Devices**, the rest of the window is disabled.
  This is where you set log and alert definitions for storage device activity if all storage devices are allowed or blocked.
  You can also determine whether you want to allow or block the Autorun feature available on some storage devices such as CD/DVD (explained in *U3 Smart Drive and Autorun Control* in *Chapter 1, Introducing SafeGuard PortProtector*).
- **Storage Types** (middle area): if you have selected the **Restrict** option for *All Storage Devices* as described in the previous paragraph, this option enables you to allow or restrict access to a storage device according to its type. For example: Removable Devices or CD/DVD Drives. The device types available for selection are built into SafeGuard PortProtector and include the following:
- Removable Media: Applies to all plug-and-play storage devices, such as Disk on Keys, Digital Camera, Portable MP3 players and so on.
- External Hard Disks
- CD/DVD Drives
- Floppy Drives
- Tape Drives

Use the *White List* to add **Approved Model**s or **Distinct Devices**. A description of the supported Device Types is provided in *Appendix B - Supported Device Types*.

For an explanation of how to define options in this window refer to *Defining Storage Control.*

3.3.6.3 Storage Control - White List Tab



The window is divided into two areas:

Approved Models (top area): This option refers to the model of a specific storage device type, such as a specific Disk On Key model.

- **Approved Distinct Devices/Media** (bottom area): This option refers to two types of groups:
- Distinct storage devices with a unique serial number, meaning an actual specific device. For example: the CEO's personal Disk On Key may be permitted to connect, while other Disk On Key devices are not.
- Approved CD/DVD media which were previously scanned and "fingerprinted".

You use both these areas to add approved storage device and media groups.

For each group, you can define the following:

- Action (Allow/ Encrypt/Read Only) – not relevant to media groups
- Permissions (Disk On Key smart functionality or File Control) – not relevant to media groups
- Log settings
- Alert settings

On the right hand side of the tab, three buttons are available:

- **New Group** ( ): use this button to add a new device group.
- **Edit Group** ( ): use this button to edit a device group.
- **Delete Group** ( ): use this button to delete a device group.

Note: This window is disabled whenever you select the **Allow** or **Block** option for All Storage Devices in the *General* tab.

For an explanation of how to define settings in this window refer to *Defining Storage Control.*

3.3.6.4 Defining Storage Control

To define Storage Control:

1 In the *Storage Control* window, click the *General* tab if it is not the active tab**.**

2 In the *Policy for All Storage Devices* section, specify whether **All Storage Devices** are **Allow(ed)** ( ), **Restrict(ed)** ( ) or **Block(ed)** ( ) by selecting your choice from the *Action* drop-down menu.

Note: Select **Allow** or **Block** when you do not want to apply granular storage device control at this point in time, but plan to define it later on. Alternatively, use this option when you wish to override existing granular definitions but want to return to them at a later time.

3 If you select **Allow** or **Block** for **All Storage Devices**, you can also specify whether device activity should be logged and/or whether alerts should be generated by checking the **Log** and/or **Alert** checkboxes.

4 If you select **Allow** or **Block** for **All Storage Devices,** there is nothing more you need to do in the *Storage Control* window and you can now skip to *Step 8: Define WiFi Control*.
The rest of the instructions in this section apply only when you select **Restrict** for **All Storage Types**.

5 In the *Action* drop-down menu, set the **Autorun Functionality** to **Allow** or **Block** (for an explanation of this functionality, refer to *U3 Smart Drive and Autorun Control* in *Chapter 1, Introducing SafeGuard PortProtector).*

6 Set permissions for **Storage Types** in the *Action* drop-down menu as follows:

- **Allow** ( ): allows all storage devices of this type.
- **Encrypt** ( ): access to this storage device type is allowed only if it is encrypted by the organization**.** If a non-encrypted device is connected, the end-user will be asked to encrypt it, as explained in *Encryption and Decryption of Removable Storage Devices* in *Chapter 9, End-User Experience*. If the end-user does not perform encryption, the device is blocked or set to read-only, depending on the definitions you have set (refer to *Defining Media Encryption* Settings). **This type of permission is available for Removable Storage Devices, External Hard Disks and for CD/DVD**. For an explanation of how end-users can perform encryption please refer to *Chapter 9, End User Experience*.

Note: In line with the "most permissive applies" rule:

If a device or media is defined as **Encrypt** in one place (for example here) and as **Allow** in another (for example in the *White List*) – the **Allow** permission will apply.

If a device or media is defined as **Encrypt** in one place (for example here) and as **Read Only** in another (for example in the *White List*) – the **Encrypt** permission will apply.

- **Read Only** ( ): allows only reading from the storage devices of this type through unblocked ports. For CDs and DVDs, assigning **Read Only** means that they cannot be used for burning.

Note: In line with the "most permissive applies" rule, if a device is defined as **Read Only** in one place (for example here) and as **Allow** in another (for example in the *White List*) – the **Allow** permission will apply.

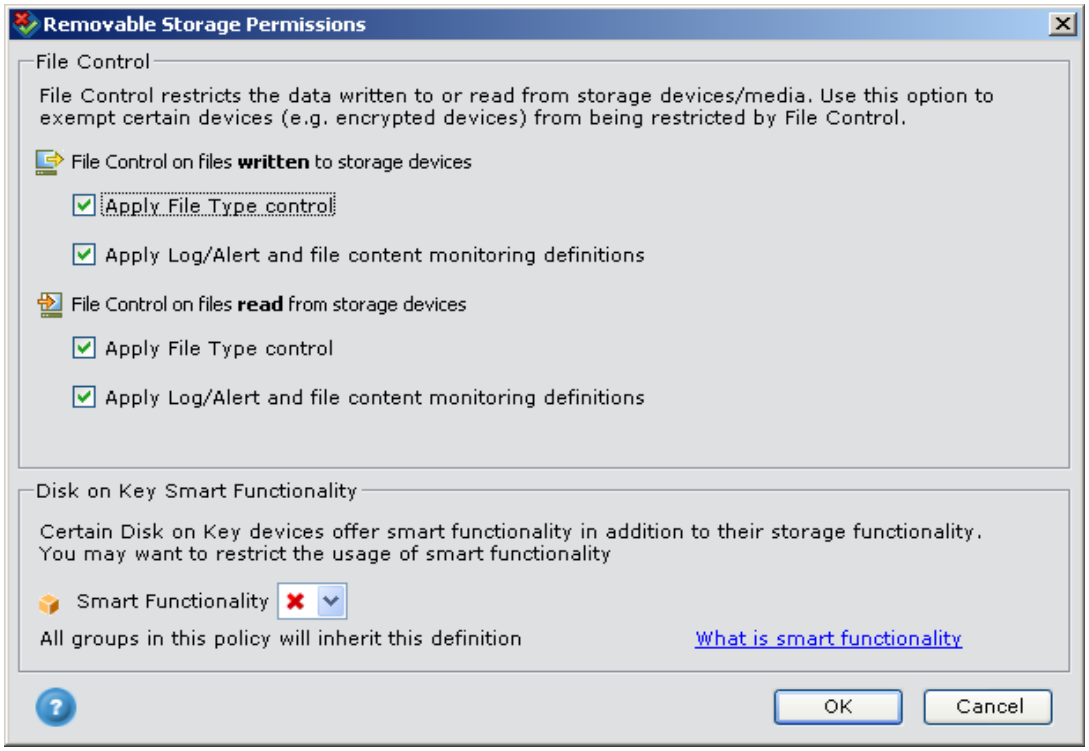
- **Restrict** ( ): all devices are blocked excluding storage devices and/or CD DVD media that you approve in the *White List* tab as described in *Approving Devices and WiFi Connections* and *Approving CD/DVD Media*. White listed CD/DVD media are allowed Read Only access in any CD/DVD drive.

3.3.6.4.1 Additional Permissions

You may set additional permissions for Removable Storage Devices, External Hard Disks and CD/DVD.

To set additional removable storage device permissions:

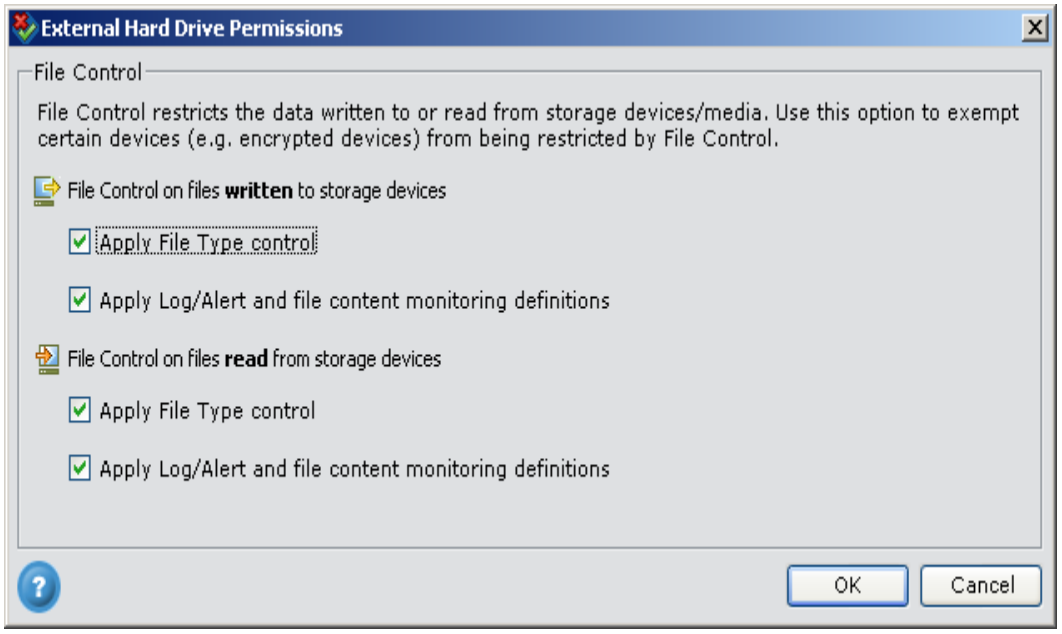
Click the **Additional Permissions** button ... For Removable Storage Devices. The *Removable Media Permissions* window opens:


Removable Storage Permissions
File Control
File Control restricts the data written to or read from storage devices/media. Use this option to exempt certain devices (e.g. encrypted devices) from being restricted by File Control.
File Control on files written to storage devices
Apply File Type control
Apply Log/Alert and file content monitoring definitions
File Control on files read from storage devices
Apply File Type control
Apply Log/Alert and file content monitoring definitions
Disk on Key Smart Functionality
Certain Disk on Key devices offer smart functionality in addition to their storage functionality. You may want to restrict the usage of smart functionality
Smart Functionality
All groups in this policy will inherit this definition
What is smart functionality
OK
Cancel

For instructions on how to set permissions, refer to *Setting Removable Storage Permissions*.

To set additional external hard disk permissions:

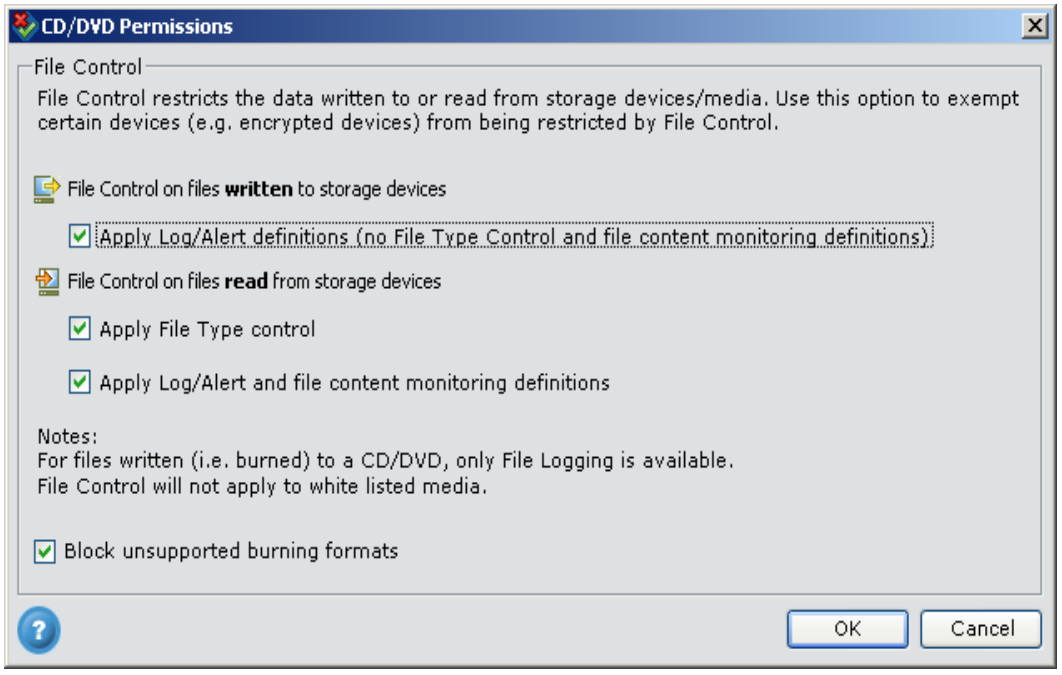
Click the **Additional Permissions** button ... For External Hard Disks. The *External Hard Disk Permissions* window opens:


External Hard Drive Permissions
File Control
File Control restricts the data written to or read from storage devices/media. Use this option to exempt certain devices (e.g. encrypted devices) from being restricted by File Control.
File Control on files written to storage devices
Apply File Type control
Apply Log/Alert and file content monitoring definitions
File Control on files read from storage devices
Apply File Type control
Apply Log/Alert and file content monitoring definitions
OK
Cancel

For instructions on how to set permissions, refer to *Setting External Hard Disk Permissions.*

To set additional CD/DVD permissions:

Click the **Additional Permissions** button ... For CD/DVD. The *CD/DVD Permissions* window opens:


CD/DVD Permissions
File Control
File Control restricts the data written to or read from storage devices/media. Use this option to exempt certain devices (e.g. encrypted devices) from being restricted by File Control.
File Control on files written to storage devices
Apply Log/Alert definitions (no File Type Control and file content monitoring definitions)
File Control on files read from storage devices
Apply File Type control
Apply Log/Alert and file content monitoring definitions
Notes:
For files written (i.e. burned) to a CD/DVD, only File Logging is available.
File Control will not apply to white listed media.
Block unsupported burning formats
OK
Cancel

For instructions on how to set permissions, refer to *Setting CD/DVD Permissions.*

3.3.6.4.1.1 Setting Removable Storage Permissions

Use these permissions to exempt removable storage devices from File Control (see *Step 7: Define File Control* in *Chapter 3, Defining Policies*) and to block smart functionality usage (see explanation below).
You may want to exempt removable storage devices from File Control in the case of encrypted devices, for example, since you know these devices to be protected. This will prevent the production of excessive logs and the need to inspect content which is safe.

The default definitions are set to **Apply** File Control on files written/read to/from storage devices and **Allow** Smart Functionality

To set removable storage permissions:

1 Set the required definitions in this window, as follows:

- **File Control:** In this section, uncheck the appropriate checkbox (*Apply File Type Control/Apply Log/Alert and Shadowing definitions*) in order to exempt files written/read to/from approved devices from File Control, as required (to subject exempted files to File Control again, check the appropriate checkbox).
- **Disk On Key Smart Functionality**: Certain Disk on Key devices, such as U3 devices, offer smart functionality in addition to their basic storage functionality. This functionality allows them to store and run applications once connected to a host computer. You may wish to limit these devices to their storage functionality only, and block the applications they carry. Do this by selecting Block ( ). All device groups belonging to this policy will inherit this definition, unless you override it with group-specific definitions as explained in *Additional Device Group Settings*.

2 Click **OK** to save and to close the *Removable Media Permissions* window.

3.3.6.4.1.2 Setting External Hard Disk Permissions

Use these permissions to exempt external hard disks from File Control (see *Step 7: Define File Control* in *Chapter 3, Defining Policies*).

The default definitions are set to **Apply** File Control to files written/read to/from storage devices.

To set external hard disk permissions:

1 In the *File Control* section, uncheck the appropriate checkbox (*Apply File Type Control/Apply Log/Alert and Shadowing definitions*) in order to exempt files written/read to/from approved devices from File Control,, as required (to subject exempted files to File Control again, check the appropriate checkbox).

2 Click **OK** to save and to close the *External Hard Disk Permissions* window.

3.3.6.4.1.3 Setting CD/DVD Permissions

Use these permissions to exempt CD/DVDs from File Control (see *Step 7: Define File Control* in *Chapter 3, Defining Policies*).

The default definitions are set to **Apply** File Control to files written/read to/from storage devices.

To set CD/DVD permissions:

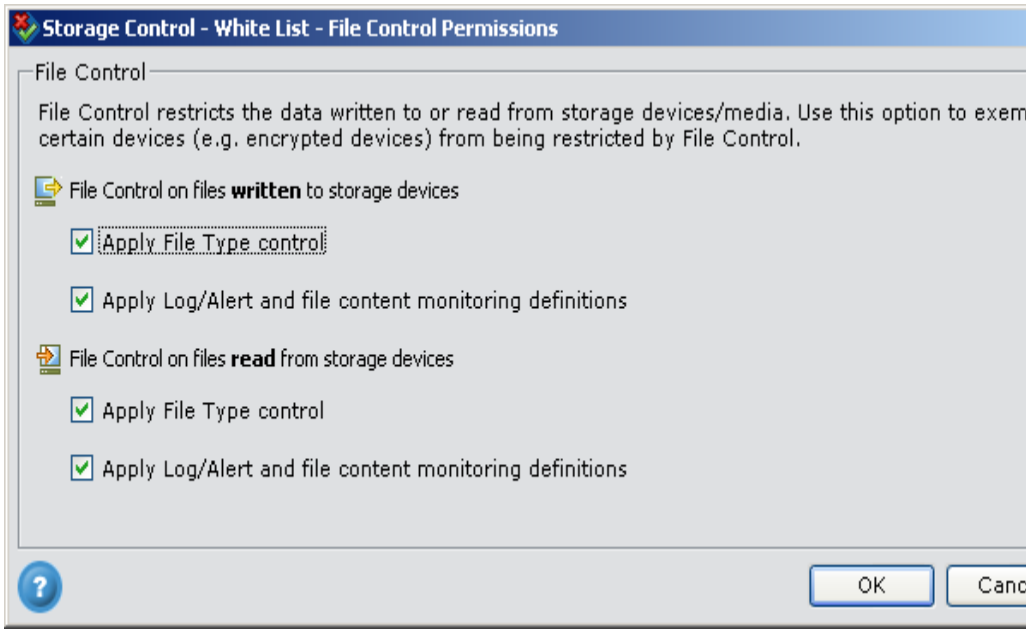
1 In the *File Control* section, uncheck the appropriate checkbox (*Apply File Type Control/Apply Log/Alert and Shadowing definitions*) in order to exempt files written/read to/from approved devices from File Control, as required (to subject exempted files to File Control again, check the appropriate checkbox).

Note:

File Control can be applied to files read from CD/DVDs but not to files written to them.

Note:

File Control will apply to white listed media.


Storage Control - White List - File Control Permissions
File Control
File Control restricts the data written to or read from storage devices/media. Use this option to exem
certain devices (e.g. encrypted devices) from being restricted by File Control.
File Control on files written to storage devices
Apply File Type control
Apply Log/Alert and file content monitoring definitions
File Control on files read from storage devices
Apply File Type control
Apply Log/Alert and file content monitoring definitions
OK
Canc

File Type *Control* for Storage White List

2 When writing to a CD/DVD, SafeGuard PortProtector can log files that meet the following three conditions:

- The burning method is Track At Once
- The file system is ISO based (i.e. ISO, ISO+JOILET, ISO+UDF)
- This is the first writing session to this CD

  Files that do not meet all three conditions will not be logged.

  Writing of files to CD/DVD that cannot be logged by SafeGuard PortProtector is blocked by default. A SafeGuard PortProtector Client message is displayed to the end-user when she/he attempts to write an unsupported format.

  If you wish to allow writing of these files, uncheck the **Block unsupported burning formats** checkbox.

3 Click **OK** to save and to close the *CD/DVD Permissions* window.

3.3.7 Step 7: Define File Control

SafeGuard PortProtector allows you to set permissions not only for storage devices, but also for the files transferred to and from these devices. This is achieved by inspecting files for their type as they are transferred to/from external storage devices. This technology allows for highly reliable classification of files by inspecting the file header contents rather than using file extensions, thus preventing users from easily bypassing the protection by renaming file extensions. With close to 200 built-in file types of all popular applications categorized into 14 file categories, policy definition has never been more fine-grained.

By inspecting both files downloaded to external storage devices and those uploaded to the protected endpoint, multiple benefits can be achieved:

- An additional protection layer to prevent data leakage
- Prevention of the introduction of viruses/malware via external storage devices
- Prevention of the introduction of inappropriate content via external storage devices, e.g. unlicensed software, unlicensed content (e.g. music and movies), non work-related content such as private pictures etc.

With this feature, you can define policies which approve/block specific file types on the inbound and outbound channels. This includes separate definitions for the inbound and outbound channels as well as support for both white list and black list methodologies.

SafeGuard PortProtector's File Control includes the following:

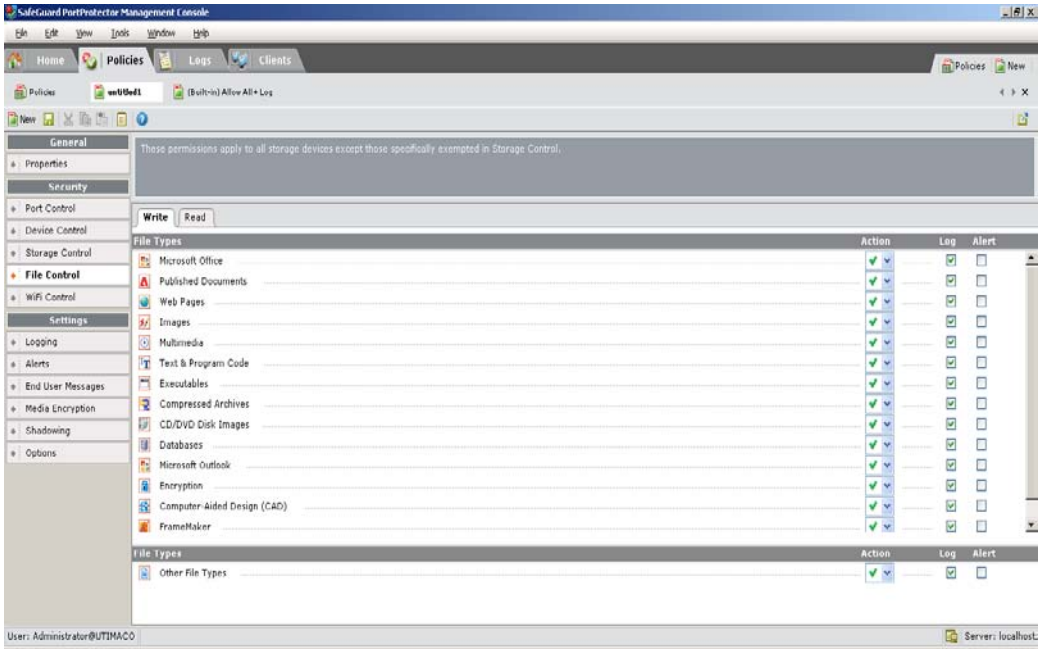
- **File Type Control** - the ability to control transfer of files according to their type.
- **File Logging** - the ability to issue logs and/or alerts upon transfer of specified file types (this replaces the file logging feature that was available in earlier versions).
- **File Shadowing** - the ability to track and collect copies of the actual files that have been moved to/from external storage devices (see

- Step 14: Define File Shadowing).

File Control is applicable to removable storage devices, external hard disks and CD/DVD.

To display the *File Control* window:

1 In the *Security* menu on the left, click the **File Control** button. The following window opens:



The *File Control* window includes two tabs, described below: the *Write* tab, which you use to specify permissions for file types written to storage devices, and the *Read* tab, which you use to specify permissions for file types read from storage devices. In these windows you also specify – for each file type - whether you wish to log or trigger alerts relating to files of each type. For a list of supported file types please refer to *Appendix C – Supported File Types*.

3.3.7.1 File Control - Write Tab

The top part of this window contains a list of supported file types. For each file type an *Action* menu allows you to set Write permissions, and checkboxes allow you to select Log and Alert settings.

The bottom part of the window allows you to set permissions and log and alert settings for other file types not specified in the supported file types.

For an explanation of how to define settings in this window refer to *Defining File Control*.

3.3.7.2 File Control - Read Tab

The top part of this window contains a list of supported file types. For each file type an *Action* menu allows you to set Read permissions, and checkboxes allow you to select Log and Alert settings.

The bottom part of the window allows you to set permissions and log and alert settings for other file types not specified in the supported file types.

For an explanation of how to define settings in this window refer to *Defining File Control*.

3.3.7.3 Defining File Control

Note: File Control applies to files written to or read from the following external storage devices: removable storage devices, external hard disks and CD/DVD drives (in the case of CD/DVD, File Control can be applied to files read from – but not to files written to – the device).

If you wish, you can exempt one or more of these storage devices from file control. This is explained in *Setting Removable Storage Permissions*, *Setting External Hard Disk Permissions* and *Setting CD/DVD Permissions*.

To define file control:

1 In the *File Control* window, click the *Write* tab.

2 For each file type, select the required permission from the *Action* menu as follows:

- **Allow** ( ): allows writing files of this type without restriction.
- **Allow & Shadow** ( ): allows writing files of this type while making a copy of each file that is moved to/from external storage devices (see *Step 14: Define File Shadowing*).

Note: Use this option with caution because it may influence both network utilization and storage resources. Preferably, you should initially apply it to small, well defined parts of your organization.

- **Block** ( ): blocks writing files of this type.

3 For each file type, check the **Log** checkbox if you want writing activities to be logged. If **Log** is checked, logs are created for each file, which can be viewed in File Logs in the Logs World (see *Chapter 5, Viewing Logs*). For a list and explanation of the fields in File Log records refer to *File Log Structure* in *Chapter 5, Viewing Logs*.

Note: Once SafeGuard PortProtector has logged transfer of a file to or from a specific device, it does not log it again unless one of the following conditions is met:

- an hour has passed since the previous logging
- the computer has been restarted
- the device has been reconnected

This is done in order to avoid multiple log records from being written when the same file is repeatedly written to the same device, such as when the end-user edits a file on a storage device and repeatedly saves it.

4 For each file type, check the **Alert** checkbox if you want writing activities to trigger an alert.

5 Repeat the steps above for each file type, as well as for Other File Types which appears in the bottom part of the window.

Note: The permissions you set for Other File Types apply to any file type that does not appear in the list in the top part of the window.

Note: The default permissions for all file types are Allow and Log (no alerts).

6 Click the *Read* tab.

7 Follow steps 2-5 described above. The only difference between the *Read* tab and the *Write* tab is that in the *Read* tab the **Inspect** option does not appear in the *Action* menu, since only outbound files are inspected.

Note: The default permissions for all file types are **Allow** (no logs or alerts).

Note: Logging files read from devices may produce an excessive number of log records during procedures such as software installations.

3.3.8 Step 8: Define WiFi Control

In addition to devices, SafeGuard PortProtector controls and monitors your WiFi connections in order to ensure that Clients use authorized, secure connections only. In the *Port Control* window, you can specify that access to a WiFi port is **Restricted**. Selecting **Restricted** enables you to define more specifically, using the **WiFi Control** window, which networks are allowed to access this port.

Note: When restricting the use of WiFi as a port, SafeGuard PortProtector monitors and regulates WiFi connections over Microsoft WZC infrastructure. Any device driver that would try to access the network card, not using WZC will be blocked. Moreover, WZC is not available on Windows 2000.

If you are using a lot of WiFi cards which enforce proprietary drivers or solely use Windows 2000 in your organization, you can only **Allow** or **Block** WiFi as a port.

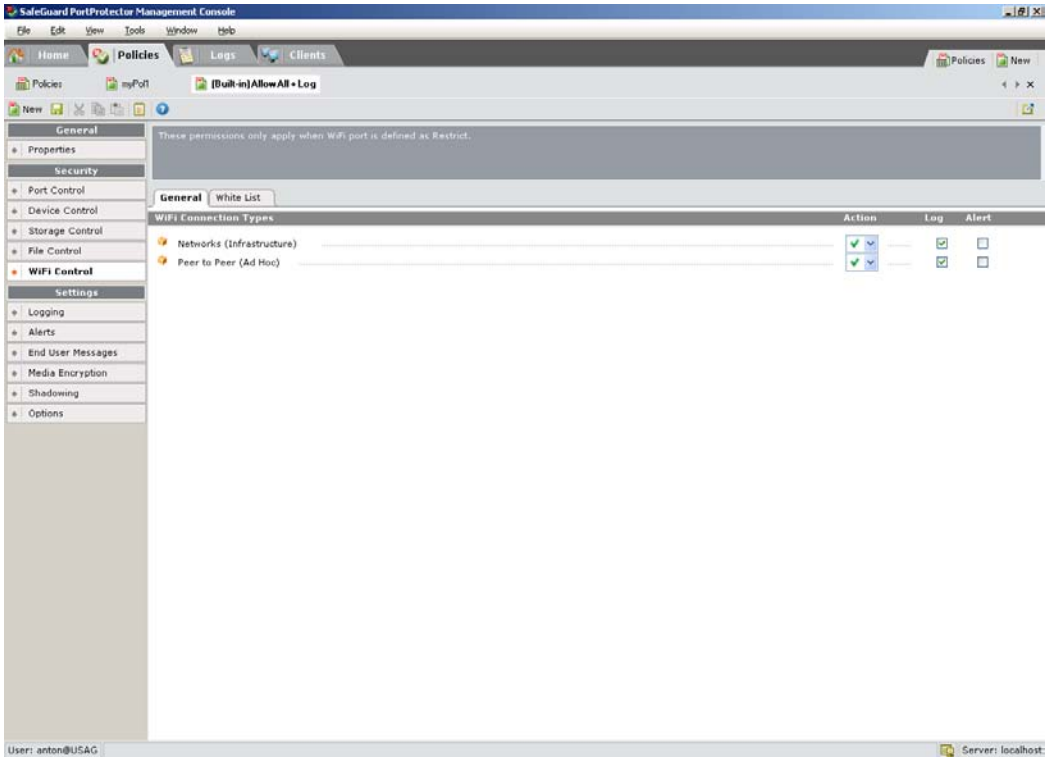
To display the *WiFi Control* window:

In the *Security* menu on the left, click the **WiFi Control** button

OR

In the *Port Control* window, click the **Define WiFi Control** link to the right of the WiFi option.

The following window opens:



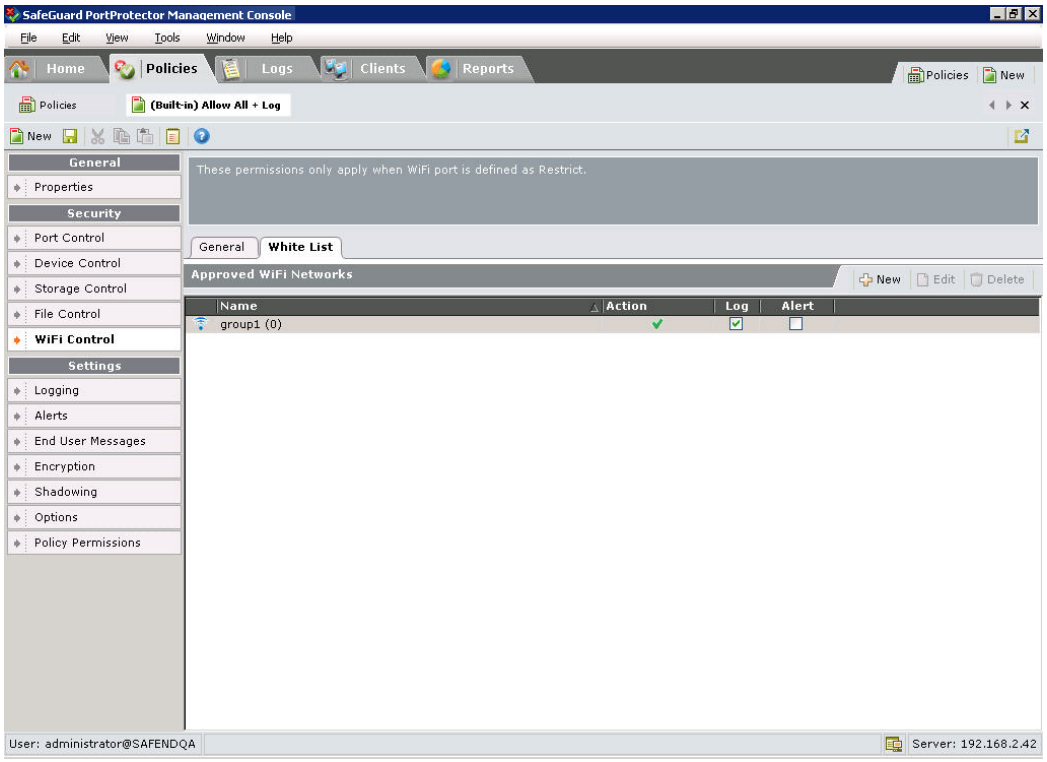
The *WiFi Control* window includes two tabs, described below: the *General* tab, which you use to specify which connection types are allowed access, and the *White List* tab, which you use to determine which specific networks are allowed access. If a connection is not defined as allowed in one of the ways described below, then it is blocked.
In addition, *WiFi Control* enables you to specify activity Log and Alert options down to the distinct network level. This means that you may choose to log connection and activity for some WiFi connections, but not to log activity for specific, allowed networks.

3.3.8.1 WiFi Control - General Tab

WiFi Connection Types: this option enables you to allow or restrict access to WiFi networks, and to allow or block WiFi peer-to-peer connections. In the case of WiFi networks, if you choose **Restrict** you may further specify which specific networks are approved.

For an explanation of how to define settings in this window refer to *Defining WiFi Control.*

3.3.8.2 WiFi Control - White List Tab



Approved WiFi Networks: This option refers to distinct networks, including their authentication and encryption properties.

On the right hand side of the tab, three buttons are available:

- **New Group** ( ): use this button to add a new device group.
- **Edit Group** ( ): use this button to edit a device group.
- **Delete Group** ( ): use this button to delete a device group.

Note: This window is disabled whenever you select the **Allow** option for Networks in the *General* tab.

Note: In cases where a network belongs to more than one group, and those groups have the same permissions, SafeGuard PortProtector will choose between the groups arbitrarily. If the groups do not have the same log and alert settings, it cannot be predicted which settings will apply.

For an explanation of how to define settings in this window refer to *Defining WiFi Control.*

3.3.8.3 Defining WiFi Control

To define WiFi Control:

1 In the *WiFi Control* window, click the *General* tab if it is not the active tab.

2 In the *WiFi Connection Types* section, in the *Action* column, set permissions for *WiFi Networks (Infrastructure)* as follows:

- **Allow** ( ): allows connection to all WiFi networks.
- **Restrict** ( ): all networks are blocked unless they are specifically approved in the *White List* tab using as described in *Approving Devices and WiFi Connections*.

3 In the *WiFi Connection Types* section, in the *Action* column, set permissions for *Peer-to-Peer (Ad Hoc)* as follows:

- **Allow** ( ): allows all peer-to-peer WiFi connections.
- **Block** ( ): blocks all peer-to-peer WiFi connections.
- In this option, more granular permissions are not available.

4 For each type of connection, check the **Log** checkbox if you want link initialization and/or activity to be logged.

5 Check the **Alert** checkbox if you want link initialization and/or activity to trigger an alert.

6 Select the **Approved Networks** to add to your White List as described in "Approving Devices and Wifi Connections".

3.3.9 Step 9: Define Global Policy Settings

Global policy settings serve as a default when you do not enter policy-specific settings. They also include log and alert definitions for events that are not policy-specific, such as tampering attempts, policy updates, protection suspension on SafeGuard PortProtector Client and more.

Note: Modifying global policy settings is optional, and if you are only evaluating SafeGuard PortProtector at this point in time it is in fact unnecessary.

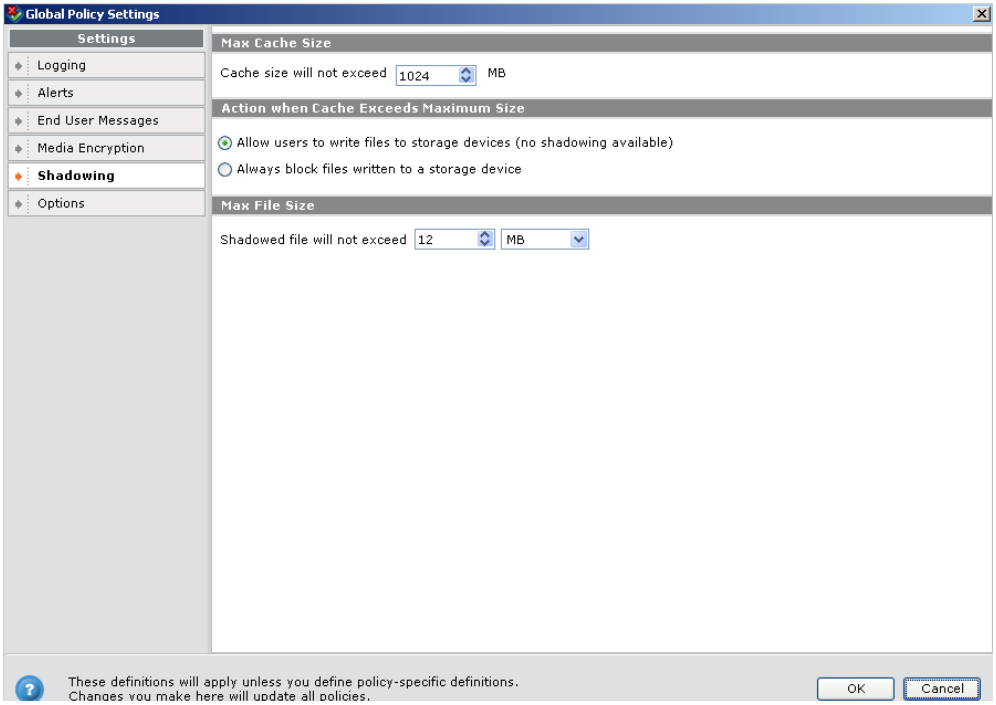
Since this step's stages are defined in the same manner as policy-specific settings, please follow the links below to modify global policy settings:

- *Defining Logging Settings*
- *Defining Alert Settings*
- *Defining End-user Messages*
- *Defining Media Encryption Settings*
- Defining Content Inspection Settings
- Defining File Shadowing Settings
- *Defining Options Settings*

3.3.9.1 Where to Define Global Policy Settings

To define global policy settings:

1 From the *Tools* menu, click **Global Policy Settings**. The *Global Policy Settings* window opens:


Global Policy Settings
Settings
Logging
Alerts
End User Messages
Media Encryption
Shadowing
Options
Max Cache Size
Cache size will not exceed 1024 MB
Action when Cache Exceeds Maximum Size
Allow users to write files to storage devices (no shadowing available)
Always block files written to a storage device
Max File Size
Shadowed file will not exceed 12 MB
These definitions will apply unless you define policy-specific definitions.
Changes you make here will update all policies.
OK
Cancel

2 You can also open this window by clicking at the top of each of the Settings windows.

3.3.10 Step 10: Define Logging

This option specifies the logging settings for the current policy, such as the frequency at which logs are sent to the SafeGuard PortProtector database from a protected endpoint, and their destination.

Each endpoint on which SafeGuard PortProtector Client is installed sends its log entries, as follows:

- immediately as the event occurs, or
- periodically, as specified below

If for any reason there is no connection between an endpoint and the SafeGuard PortProtector Management Server, log entries are accumulated on the endpoint and sent once communication is renewed.

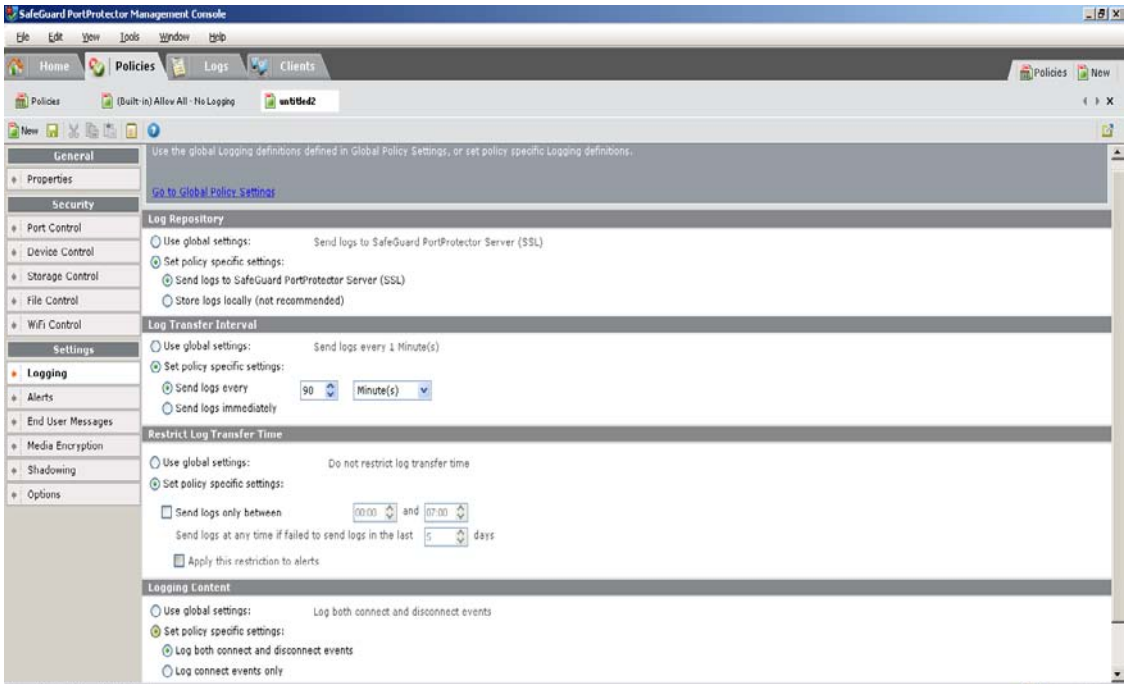
You also have the option to define whether disconnect events are logged or not.

Note: Additional, general system logging settings can be specified in the Administration window, as described in *Configuring Logs and Alerts Tab Settings* in *Chapter 7, Administration*.

Logging settings are defined in the *Logging* settings window.

To open the *Logging* settings window:

In the *Settings* menu on the left side of the main window, click **Logging**. The *Logging* window is displayed, as shown below:


SafeGuard PortProtector Management Console
File Edit View Tools Window Help
Home
Policies
Logs
Clients
Policies
New
Policies
(Built-in) Allow All - No Logging
untitled2
New
General
Properties
Security
Port Control
Device Control
Storage Control
File Control
WiFi Control
Settings
Logging
Alerts
End User Messages
Media Encryption
Shadowing
Options
Use the global Logging definitions defined in Global Policy Settings, or set policy specific Logging definitions.
Go to Global Policy Settings
Log Repository
Use global settings:
Send logs to SafeGuard PortProtector Server (SSL)
Set policy specific settings:
Send logs to SafeGuard PortProtector Server (SSL)
Store logs locally (not recommended)
Log Transfer Interval
Use global settings:
Send logs every 1 Minute(s)
Set policy specific settings:
Send logs every
90
Minute(s)
Send logs immediately
Restrict Log Transfer Time
Use global settings:
Do not restrict log transfer time
Set policy specific settings:
Send logs only between
00:00
and
07:00
Send logs at any time if failed to send logs in the last
5
days
Apply this restriction to alerts
Logging Content
Use global settings:
Log both connect and disconnect events
Set policy specific settings:
Log both connect and disconnect events
Log connect events only

3.3.10.1 Defining Logging Settings

Note: In each section of this window you may choose to use the Global Policy Settings by selecting the **Use global settings** radio button (to view or edit Global Policy Settings, click Go to Global Policy Settings at the top of the window).

The window contains the following sections:

- **Log Repository:** the settings in this section determine where logs are stored.
- **Log Transfer Interval:** the settings in this section determine whether logs are sent immediately or periodically.
- **Restrict Log File Transfer:** the settings in this section enable you to restrict log and alert transfers to the Management Server to specific hours.
- **Logging Content:** the settings in this section determine whether both connect and disconnect events, or only connect events, are logged.
- **Track offline use of devices:** this section enables you to track usage of encrypted devices by authorized end-users when they are not connected to the organizational network (see *Tracking Offline Use of Encrypted Devices* in *Chapter 8, End user experience).*

Note: This section appears only in the *Global Policy Settings* window.

To define logging settings:

1 In the **Log Repository** section, click the **Set Policy Specific Settings** radio button (ignore this step if you are defining Global Policy settings).

2 Select one of the following radio buttons:

- **Send logs to SafeGuard PortProtector Server (SSL):** click this option to send logs to SafeGuard PortProtector Management Server using the secure SSL protocol.
- **Store logs locally (not recommended)**: despite it not being recommended, click this option to store log records locally on the endpoint and never send them to the Management Server.

3 In the Log Transfer Interval section, click the Set Policy Specific Settings radio button.

4 Select one of the following radio buttons:

- **Send logs every:** click this option to send logs periodically. Set the number and the unit to specify the required interval.
- **Send logs immediately:** click this option to send logs as soon as an event occurs.

Important:

Take extra care while configuring the *Logs Transfer Interval* in order not to burden your network and endpoints with excessive log sending.

Consider the following:

- The number of endpoints in your network
- The number of expected events from each endpoint (Client and File logs)
- The level of need for "real time" logs information in the Management Console

During installation, the default log interval is set to 90 minutes. In the case of large scale deployments, please consult Support in order to optimize your settings.

5 In the Restrict Log Time Transfer section, click the Set Policy Specific Settings radio button.

6 Check the **Send logs only between** checkbox and set the desired timeframe for sending logs.

7 Select the number of days that, if passed without sending logs, should enable sending of logs at any time.

8 Check the checkbox to **apply this restriction to alerts** (alert logs are normally sent immediately. If you check this checkbox they will be sent at the same time as the logs. The alert event, such as email notification, will occur immediately).

9 In the Logging Content section, click the Set Policy Specific Settings radio button.

10 Select one of the following radio buttons:

- **Log both connect and disconnect events:** click this option to log disconnect events as well as connect events.
  For all allowed devices, storage devices and WiFi links, a log entry is recorded when the device is connected or disconnected. Logging disconnect events enables you to use the logs to determine when and for how long a device was connected.
- **Log connect events only:** click this options if you only want to log connect events.

11 In the **Track Offline Use of Devices** section, check the checkbox in order to log offline use of encrypted devices.

Note:

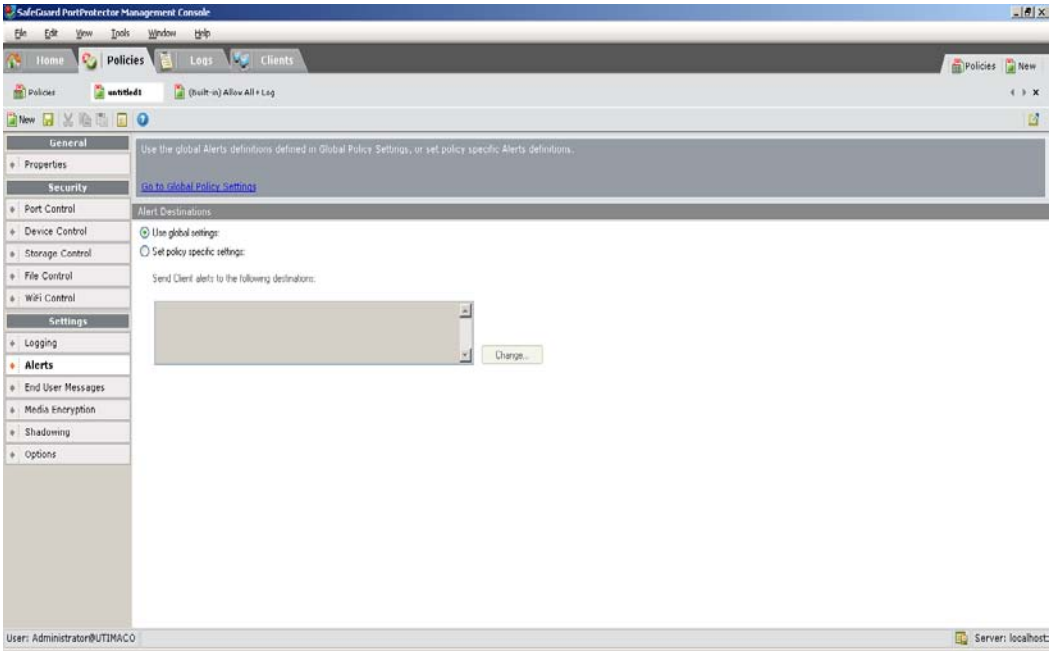
This section appears only in the *Global Policy Settings* window.

3.3.11 Step 11: Define Alerts

The *Alerts* settings window is where you select Client alert destinations.

To open the *Alerts* settings window:

In the *Settings* menu on the left side of the main window, click **Alerts**. The *Alerts* window is displayed, as shown below:



3.3.11.1 Defining Alert Settings

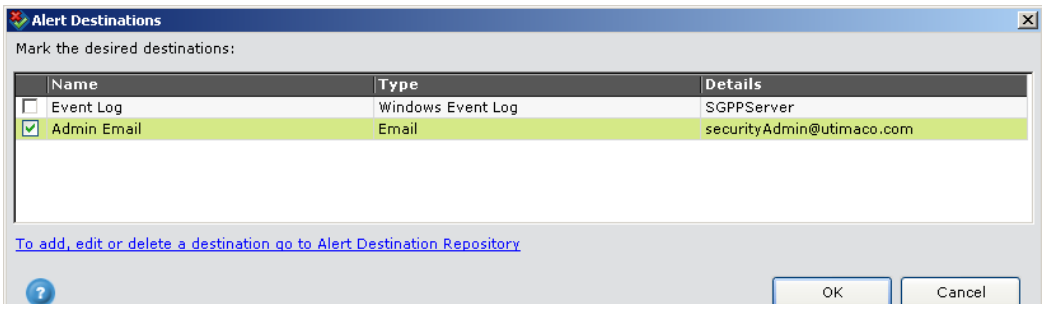
Note: You may choose to use the Global Policy Settings by selecting the **Use global settings** radio button (to view or edit global Policy Settings, click Go to Global Policy Settings at the top of the window).

To define alert settings:

1 In the **Client Events** section, define which administration and tampering events you wish to log/alert (ignore this step if you are not defining Global Policy settings).

2 Select the **Set policy specific settings** radio button. If alert destinations have been defined in the past, they appear in the destination list. If not, the list is blank (ignore this step if you are defining Global Policy settings).

3 Click **Change**. The *Alert Destinations* window opens, displaying all available destinations defined in the Alert Destination Repository (refer to Alert Destination Repository in Chapter 7, Administration).



4 Select or de-select the required destinations and click **OK**.

Note: To add, edit or delete a destination, refer to Alert Destination Repository in *Chapter 7, Administration*.

3.3.12 Step 12: Define End User Messages

Once a SafeGuard PortProtector policy is applied, SafeGuard PortProtector Client displays an event message to the end-user in various situations, such as when an attempted violation of the policy is detected or end-user action is required

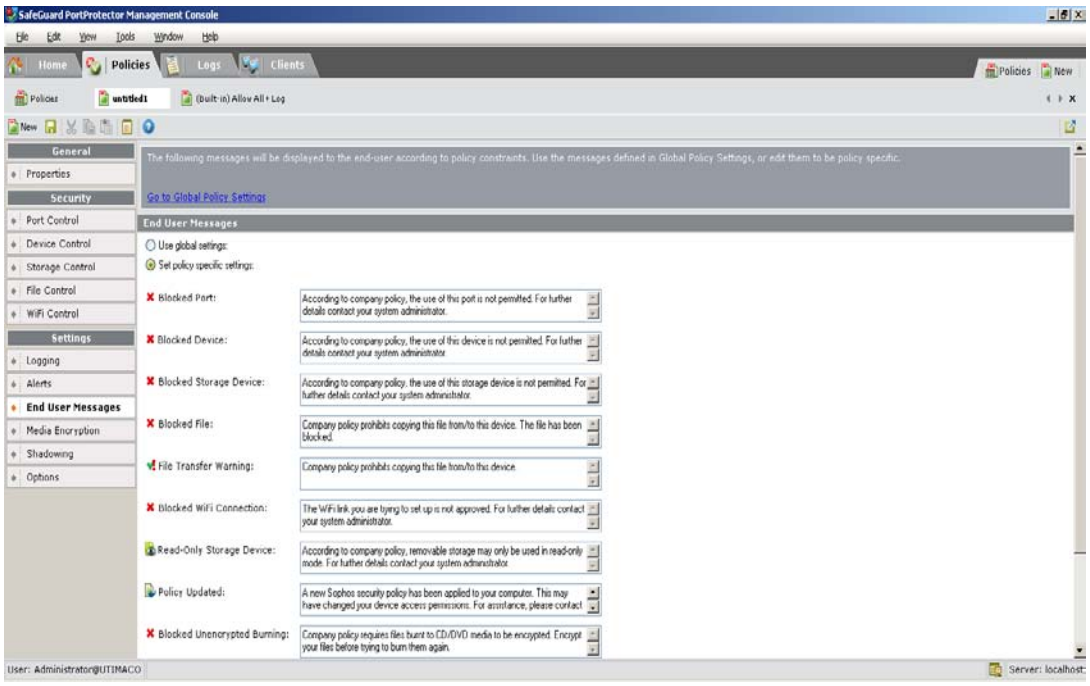
SafeGuard PortProtector Client comes with default messages which you can edit using the **End-user Messages** option in the *Settings* menu, on the left side of the main window.

Note: You may refer to the *SafeGuard PortProtector Client Messages* section for a description of how and when these messages appear on the endpoints.

End-user message settings are defined in the *End-user Messages* settings window.

To open the *End User Messages* settings window:

In the *Settings* menu left side of the main window, click **End User Messages**. The *End User Messages* window is displayed, as shown below:



3.3.12.1 Defining End-user Messages

Note: You may choose to use the Global Policy Settings by selecting the **Use global settings** radio button (to view or edit Global Policy Settings, click Go to Global Policy Settings at the top of the window).

To define end-user message settings:

1 Select the **Set policy specific settings** radio button (ignore this step if you are defining Global Policy settings).

2 Edit the messages as follows:

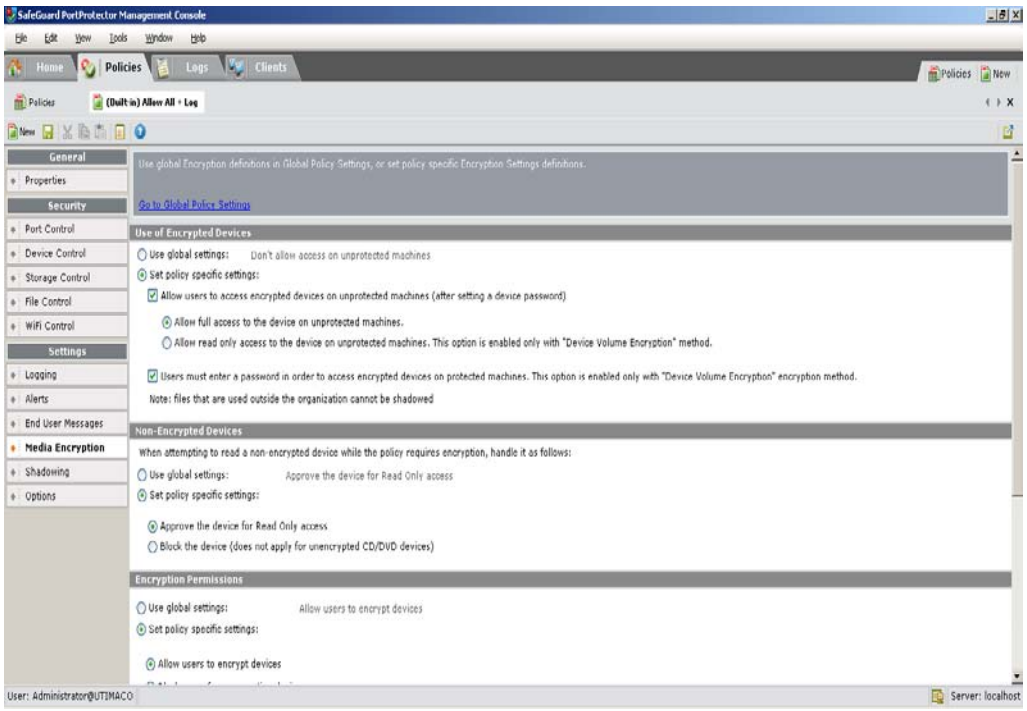
- **Blocked Port:** This message appears when a computer tries to initialize a port that is **blocked**. For built-in ports, this message appears when the endpoint computer reboots, and tries to initialize the port. It also appears when an adapter for this port is connected to the endpoint.
- **Blocked Device:** This message appears when an attempt is made to connect an unapproved device through a **restricted** port.
- **Blocked Storage Device:** This message appears when an attempt is made to connect an unapproved storage device.
- **Blocked File:** This message appears when the end-user attempts to write/read a file whose type is blocked to/from a storage device.
- **File Transfer Warning:** This message appears when writing a file with sensitive content to a storage device.
- **Blocked WiFi Connection:** This message appears when an attempt is made to connect to an unapproved WiFi connection.
- **Read Only Storage Device:** This message appears when a storage device that is set to **Read Only** is connected. This message indicates that you can read from this storage device, but not write to it.
- **Policy Updated:** This message appears when a new policy is applied to the endpoint.
- **Format Encrypted Device:** This message appears when the policy requires that removable storage media be encrypted and a non-encrypted device is detected (refer to *Encrypting a Device* in *Chapter 9, End-user Experience*).
- **Blocked hardware Key Logger:** This message appears when an attempt is made to connect a hardware key logger, and hardware key loggers are set to **Blocked**.

3.3.13 Step 13: Define Media Encryption

Encryption settings determine the system's behavior when removable storage device permissions are set to Encrypt. Encryption settings are defined in the *Media Encryption* settings window.

To open the *Media Encryption* settings window:

In the *Settings* menu on the left side of the main window, click **Media Encryption**. The *Media Encryption* settings window is displayed, as shown below:


SafeGuard PortProtector Management Console
File Edit View Tools Window Help
Home Policies Logs Clients
Policies New
(Built-in) Allow All + Log
General
Properties
Security
Port Control
Device Control
Storage Control
File Control
WiFi Control
Settings
Logging
Alerts
End User Messages
Media Encryption
Shadowing
Options
Use global Encryption definitions in Global Policy Settings, or set policy specific Encryption Settings definitions.
Go to Global Policy Settings
Use of Encrypted Devices
Use global settings: Don't allow access on unprotected machines
Set policy specific settings:
Allow users to access encrypted devices on unprotected machines (after setting a device password)
Allow full access to the device on unprotected machines.
Allow read only access to the device on unprotected machines. This option is enabled only with "Device Volume Encryption" method.
Users must enter a password in order to access encrypted devices on protected machines. This option is enabled only with "Device Volume Encryption" encryption method.
Note: files that are used outside the organization cannot be shadowed
Non-Encrypted Devices
When attempting to read a non-encrypted device while the policy requires encryption, handle it as follows:
Use global settings: Approve the device for Read Only access
Set policy specific settings:
Approve the device for Read Only access
Block the device (does not apply for unencrypted CD/DVD devices)
Encryption Permissions
Use global settings: Allow users to encrypt devices
Set policy specific settings:
Allow users to encrypt devices
User: Administrator@UTIMACO
Server: localhost

3.3.13.1 Defining Media Encryption Settings

Note: In each section of this window you may choose to use the Global Policy Settings by selecting the **Use global settings** radio button (to view or edit Global Policy Settings, click Go to Global Policy Settings at the top of the window).

The window contains the following sections:

- **Use of Encrypted Devices:** the settings in this section determine whether the users may access organizationally-encrypted removable storage devices on non-organizational computers, with full access or read only access (refer to *Chapter 9, End-user Experience*). Also, whether one can access encrypted removable storage devices even within the organization: i.e., a password is required for access (refer to*Accessing Encrypted Devices Online*).
- **Non-encrypted Devices:** in this section you can determine behavior when the policy requires encryption and a non-encrypted device is detected; the device may either be blocked, or permitted Read Only access.

- **Encryption Method:** In this section, you determine the method for encrypting removable storage devices, which influence the method in which permitted users will access the encrypted storage devices outside the organization, as described in *Encryption and Decryption of Removable Storage Devices* in *Chapter 9, End-User* Experience. The difference between the two encryption methods is described in *Media Encryption Methods.*

To define encryption settings:

1 In the **Use of Encrypted Devices** section, click the **Set Policy Specific Settings** radio button (ignore this step if you are defining Global Policy settings).

2 If you want to allow users access to organizationally-encrypted devices when away from the organizational network, check the **Allow users to access encrypted devices on unprotected machines** checkbox.

3 Select the appropriate radio button to choose whether the user will have full access or read only access.

4 If you want to restrict users access to encrypted devices within the organizational network, check **Users must enter password in order to access encrypted devices on protected machines**.
This option is enabled, only if you choose both **Allow users to access encrypted devices on unprotected machines** and **Device Volume Encryption** for *Encryption Method*.

5 In the Non-encrypted Devices section, click the Set Policy Specific Settings radio button.

6 Select the appropriate radio button depending on whether you wish to block non-encrypted devices or to allow the users read-only access to such devices.

7 Select the appropriate radio button to determine whether to use Device **Partition Encryption** (default) **Device Volume Encryption** to determine the method for allowing offline access to removable storage devices by permitted users.

Attention System Administrator:
End-users whose effective policy requires encryption of removable storage devices should be made aware of the instructions in *Encryption and Decryption of Removable Storage Devices* in *Chapter 9, End-user Experience*, since their Client may display messages that require them to encrypt removable storage devices.

3.3.13.1.1 Media Encryption Methods

SafeGuard PortProtector offers two methods for encrypting removable storage devices. The encryption method used will influence the way in which permitted users will access the encrypted storage devices outside the organization, as described in *Encryption and Decryption of Removable Storage Devices* in *Chapter 9, End-User* Experience.

- **Device Volume Encryption:** This encryption method enables offline access to storage devices by permitted users **without** requiring them to have local administration permissions. However, the process of accessing files by the user is slightly less intuitive when compared with the **Partition Encryption** option (described below). The removable storage device shows two files; the Access Secure Data utility and a container of the encrypted files.

Note:
Do not delete the container of the encrypted files from the removable storage device. Deleting the container will delete all information stored in it.

- **Device Partition Encryption (default):** This encryption method enables access to storage devices by permitted users outside the organization, **but** requires them to have local administration rights on the unprotected machine. The process of accessing files by the user is simpler than when using the **Device Volume Encryption** option (described above).

Note:
The above only applies to removable storage devices. The Device Volume Encryption method is applied by default to CD/DVD and external hard disks.

3.3.14 Step 14: Define File Shadowing Settings

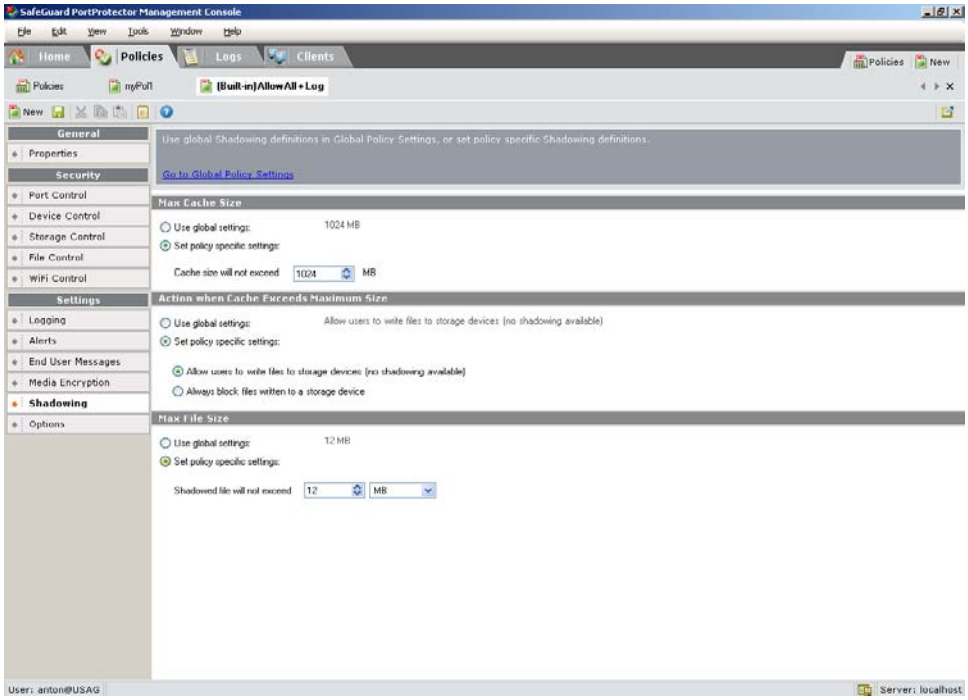
File Shadowing provides the ability to track and collect copies of files that have been moved to/from external storage devices, and provides security officers the ability to pinpoint and identify security breaches and to analyze forensic evidence, assess its severity and take appropriate action.

The Shadowed files are sent securely from the endpoints to the server and stored in a central repository. These files are available for review by authorized administrators that have the **View Shadow Files** permission. The shadowed files are stored under their original file names and in their original format.

One or more network shares can be defined by an administrator as the File Shadowing central repository. If multiple network shares are defined, then a load balancing algorithm is used to verify that utilization is distributed evenly among all the shares.

To open the File Shadowing settings window:

In the *Settings* menu on the left side of the main window, click **Shadowing**. The File Shadowing settings window is displayed, as shown below:



3.3.14.1 Defining File Shadowing Settings

Note:

In each section of this window you may choose to use the Global Policy Settings by selecting the **Use global settings** radio button (to view or edit Global Policy Settings, click *Go to Step 9: Define Global Policy Settings* at the top of the window).

This window contains the following sections:

- **Max Cache Size:** The settings in this section determine the maximum size of the local cache repository into which the files are shadowed. Much like the logging mechanism, shadowed files are cached on the local protected machine until they can be relayed to a server.

Note: More storage space may be required in this local cache for laptops since, unlike desktops, they tend to function for considerable portions of the time outside the organizational network.

- **Action when Cache Exceeds Maximum Size:** The settings in this section determine the actions to be taken by SafeGuard PortProtector when the local cache exceeds the size that you defined in the **Max Cache Size** area.
- **Max File Size:** This area determines the maximum size of each file to be shadowed. Files that exceed this size will not be shadowed.

To define File Shadowing settings:

1 In the **Max Cache Size** section, in the **Cache size will not exceed** field, specify the size in MBs of the local cache. If this cache becomes full, SafeGuard PortProtector behaves according to the actions described above.

2 In the **Action when Cache Exceeds Maximum Size** area, select one of the following two radio buttons:

- **Allow users to write files to storage devices (no shadowing available):** If the local cache (defined above) becomes full, then SafeGuard PortProtector allows all files written to the storage device.
- **Always block files written to a storage device:** If the local cache (defined above) becomes full, then SafeGuard PortProtector **blocks all files** written to the storage device. By choosing this option, you ensure that no files are transferred from the protected machine without being shadowed.

3 In the **Max File Size** section, in the **Shadowed file will not exceed** field, specify the size in MBs of the largest file to be shadowed. Larger files will not be shadowed.

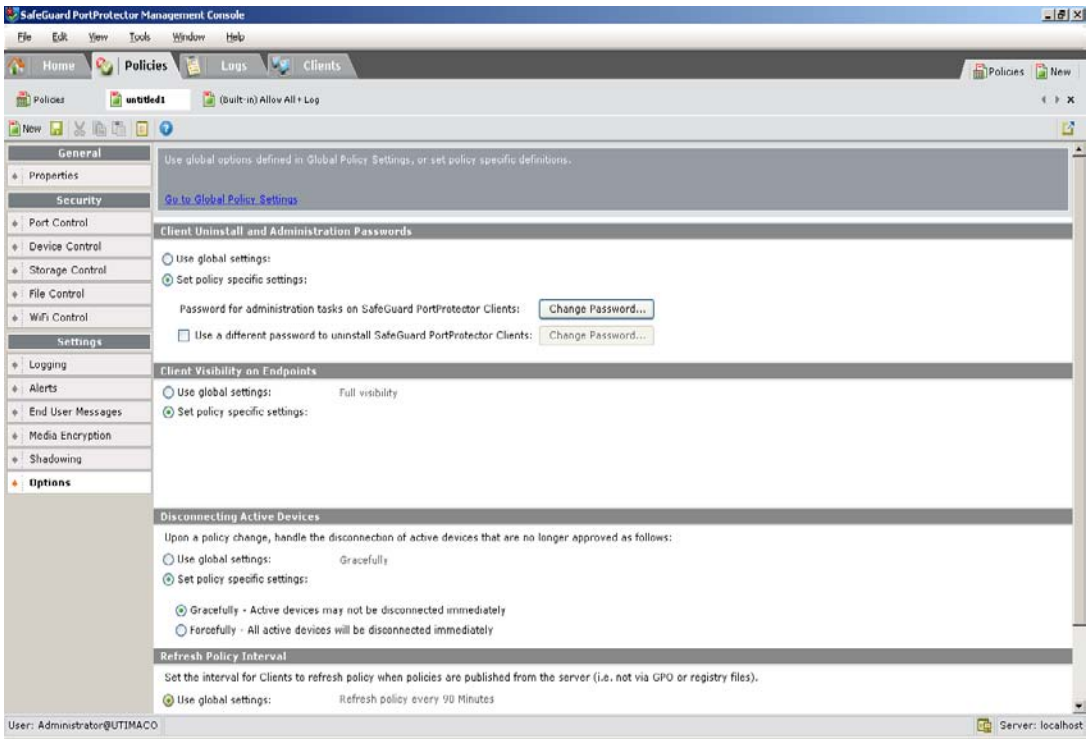
3.3.15 Step 15: Define Options

The **Options** aspect of a policy enables you to define several behavioral aspects of SafeGuard PortProtector Client on the endpoints. These comprise password settings, tray icon visibility settings and definitions of methods for disconnecting active devices when this becomes necessary.

Option settings are defined in the *Options* settings window.

To open the *Options* settings window:

In the *Settings* menu on the left side of the main window, click **Options**. The *Options* window is displayed, as shown below:


SafeGuard PortProtector Management Console
File Edit View Tools Window Help
Home Policies Logs Clients
Policies New
Policies untitled1 (Built-in) Allow All + Log
New
General
Properties
Security
Port Control
Device Control
Storage Control
File Control
WiFi Control
Settings
Logging
Alerts
End User Messages
Media Encryption
Shadowing
Options
Use global options defined in Global Policy Settings, or set policy specific definitions.
Go to Global Policy Settings
Client Uninstall and Administration Passwords
Use global settings:
Set policy specific settings:
Password for administration tasks on SafeGuard PortProtector Clients:
Change Password...
Use a different password to uninstall SafeGuard PortProtector Clients:
Change Password...
Client Visibility on Endpoints
Use global settings: Full visibility
Set policy specific settings:
Disconnecting Active Devices
Upon a policy change, handle the disconnection of active devices that are no longer approved as follows:
Use global settings: Gracefully
Set policy specific settings:
Gracefully - Active devices may not be disconnected immediately
Forcefully - All active devices will be disconnected immediately
Refresh Policy Interval
Set the interval for Clients to refresh policy when policies are published from the server (i.e. not via GPO or registry files).
Use global settings: Refresh policy every 90 Minutes
User: Administrator@UTIMACO
Server: localhost

3.3.15.1 Defining Options Settings

Note: In each section of this window you may choose to use the Global Policy Settings by selecting the **Use global settings** radio button (to view or edit Global Policy Settings, click Go to Global Policy Settings at the top of the window).

The window contains the following sections:

- ***Client Uninstall Password*:** the settings in this section determine the passwords to be used for administering and/or uninstalling SafeGuard PortProtector Client.
- ***Client Visibility on Endpoints*:** the settings in this section determine if and when SafeGuard PortProtector Client tray icon and event messages are displayed.
- ***Disconnecting Active Devices*:** the settings in this section determine the method SafeGuard PortProtector uses to disconnect devices which were previously but are no longer approved.
- ***Refresh Policy Interval:*** The settings in this section determine the interval for Clients to refresh their policy when policies are distributed directly from the Management Server (i.e. Policy Server).

Note: This section appears in the *Options* page only when using the Polciy Server for policy distribution (i.e. alone, or in addition to GPO or registry files).

3.3.15.1.1 Client Administration Password

This is the password for performing administration tasks on SafeGuard PortProtector Clients, which include suspending and uninstalling the Client. You set it in the *Administration Password* window.

To open the window:

1 In the Clients Uninstall Password section, click the **Set Policy Specific Settings** radio button (ignore this step if you are defining Global Policy settings.

2 Click the Change Password button next to Password for performing administration tasks on SafeGuard PortProtector Client. The Administration Password window opens:

3.3.15.1.1.1 Defining Client Administration Password

To define a Client administration password:

1 In this window, enter the password for performing administration tasks on SafeGuard PortProtector Clients and confirm it. The password must adhere to the organization's password rules.

2 Click **OK**.

3.3.15.1.2 Client Uninstall Password

This is the password for uninstalling SafeGuard PortProtector Clients from endpoints, if you want to use a different password from the administration password. You set it in the *Uninstall Password* window.

To open the window:

In the *Clients Uninstall Password* section, check the checkbox next to Use a different password to uninstall SafeGuard PortProtector Client from endpoints.

Click the adjacent **Change Password** button. The *Uninstall Password* window opens:

3.3.15.1.2.1 Defining Client Uninstall Password

1 In this window, enter the password for uninstalling SafeGuard PortProtector Clients from endpoints and confirm it. The password that you set must adhere to the organization's password rules.

2 Click **OK**.

Note: Upon product installation both passwords are set to "**Password1**". Since the password is one of the foundations for the tampering resistance of the Client, it is highly recommended that you change it as soon as you start deploying the product in a production environment.

3.3.15.1.3 Defining Client Visibility on Endpoints

The settings in this section determine if and when SafeGuard PortProtector Client tray icon and event messages are displayed.

1 In the *Client Visibility on Endpoints* section, click the **Set policy specific settings** radio button.

2 Select one of the following radio buttons:

- **Full visibility:** if you select this option, the SafeGuard PortProtector icon is always displayed in the tray, even while SafeGuard PortProtector Client is idle, and event messages are always shown. In this case the end-user is always aware of SafeGuard PortProtector.
- **Partial visibility**: if you select this option, the SafeGuard PortProtector icn is hidden while the Client is idle. When an event occurs, the icon and the event message are shown briefly, and then disappear.
- **Stealth mode:** if you select this option, the SafeGuard PortProtector icon and event messages are never shown. You may want to use this option when you do not want users to be aware of SafeGuard PortProtector on their computers.

3.3.15.1.4 Defining Disconnection of Active Devices

In some cases, a device may be connected to a computer to which a new policy, specifying that this device is no longer approved, is applied. In such cases, SafeGuard PortProtector Client calls upon the operating system and requests that it disconnect the device. Occasionally, when the device is in use, the operating system may fail to do so. The settings in this section determine the method SafeGuard PortProtector uses on these occasions to disconnect the no longer approved device.

1 In the *Disconnecting Active Devices* section, click the **Set policy specific settings** radio button.

2 Select one of the following radio buttons:

- **Gracefully:** if you select this option, SafeGuard PortProtector does not disconnect devices that the operating system fails to disconnect. SafeGuard PortProtector Client will try to disconnect the device again later and/or will block it following the next reboot.
- **Forcefully**: if you select this option, SafeGuard PortProtector disconnects the device immediately, disregarding the operating system and disconnecting any communication channel between the device and the computer. On very rare occasions, this may render unusable some data that was transferred to or from this device at the time of the disconnection, or the device itself, due to data corruption.

Note: We recommend that in all cases you notify users ahead of time of the fact that certain devices will no longer be allowed.

Note: In the case of WiFi links, when a new policy applied to a Client dictates that an existing link should be blocked, the link is disconnected forcefully.

3.3.15.1.5 Defining Refresh Policy Interval

Note: This section will appear in the *Options* page only if you are using the Policy server for policy distribution.

When policies are published to Clients directly from the Management Server (Policy Server distribution option), you need to set the interval for the Client to check for an updated policy. Use this section to set the interval.

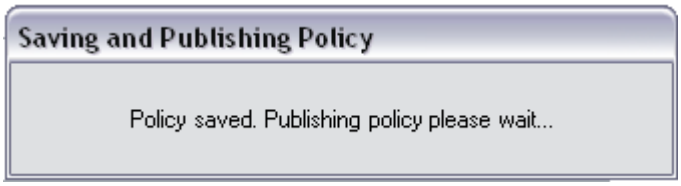
3.3.16 Step 16: Save and Publish the Policy

All new policies and all modifications to a policy should be saved. A policy may be saved under its existing name or with a new name (save a policy under a new name when it is a new policy, or when you want to save a copy of an existing policy). Saving a policy also publishes it as a GPO in Active Directory or as a registry file, if you have selected one of these methods for policy distribution (Refer to *Overview* in *Chapter 4, Distributing Policies* for more information).

3.3.16.1 Saving a Policy under its Existing Name

To save an existing policy under the same name:

From the *File* menu, select **Save and Publish**, or click the Save and Publish ( ) icon from the toolbar. The following window appears:



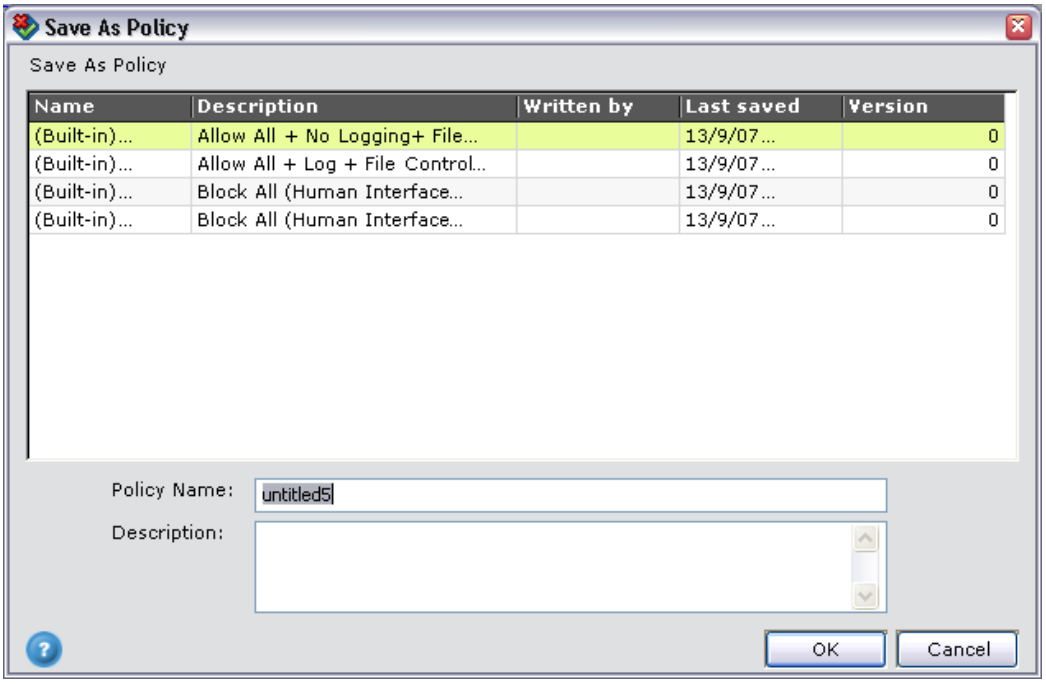
The policy is saved and published.

3.3.16.2 Saving a Policy under a New Name

You can save a policy under a new name, with a new description. This is done in the *Save As Policy* window.

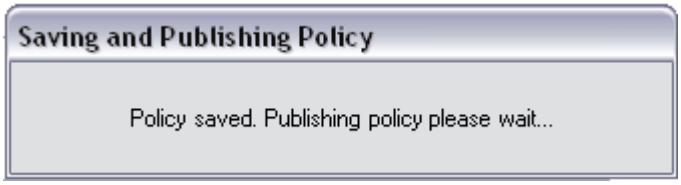
To open the Save As Policy window:

From the *File* menu, select **Save As**. A list of the existing policies is displayed in the following window:



3.3.16.2.1 Entering Policy Details

Edit the **Policy Name** (required) and **Description** (optional) fields and click **OK**. The following window appears:

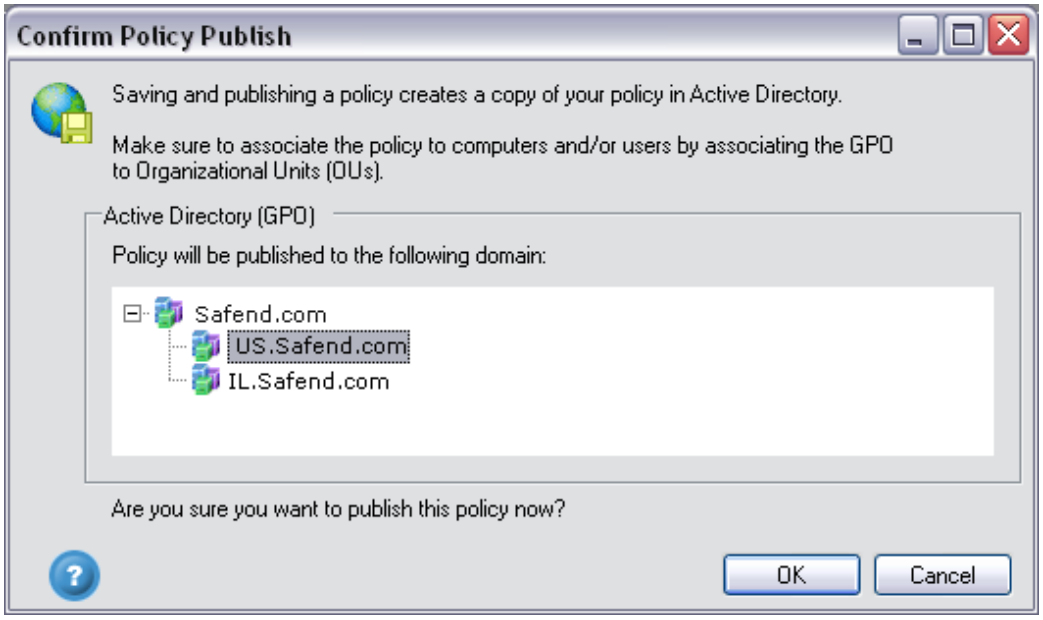


The policy is saved and published.

Note: If you save a policy with a new name, and are using Active Directory to distribute policies, the new GPO that is created has no link to the required organizational unit. Until you link the new GPO to the organizational unit, the previous policy applies.

3.3.16.3 Confirming Publish Domain

If you asked to enable domain selection when you publish a policy (refer to Publishing Method in *Chapter 7, Administration*), the *Confirm Policy Publish* window opens when you save a policy:

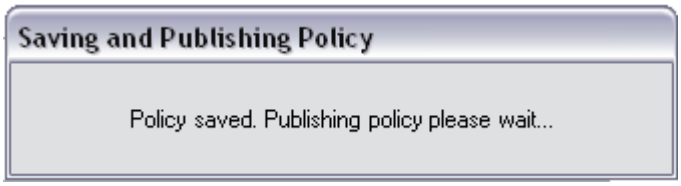

Confirm Policy Publish
Saving and publishing a policy creates a copy of your policy in Active Directory.
Make sure to associate the policy to computers and/or users by associating the GPO to Organizational Units (OUs).
Active Directory (GPO)
Policy will be published to the following domain:
Safend.com
US.Safend.com
IL.Safend.com
Are you sure you want to publish this policy now?
OK
Cancel

3.3.16.3.1 Confirm Policy Publish

The window displays the domains available in your organizational forest. You may publish the policy to the required domain.

To confirm publishing policy to the selected required domain:

Select the domain to which you wish to publish the policy and click **OK**. The following window appears:



The policy is saved and published.

If you click **Cancel**, the policy is not published (meaning no GPO or registry file is created) and is only saved in the database.

Note: If you are using Active Directory, saving and publishing a policy creates a copy of the policy (GPO) in Active Directory. Make sure to associate the policy to computers and/or user groups by associated the GPO to the required Organizational Unit.

3.4 Approving Devices and WiFi Connections

The explanations in the following sections refer to adding approved devices to the *Device Control* White List and adding approved storage devices to the *Storage Control* White List. Where differences exist between adding storage and non-storage devices, they are pointed out and explained.

Explanations on how to add approved WiFi networks can be found in *Adding WiFi Connections.*

SafeGuard PortProtector provides you with three levels of permissions:

- **Devices Types and Storage Types:** This option, explained above, enables you to allow or restrict access to an endpoint according to the type of device that is connected. For example: Removable Media, Network Adapters, Human Interface devices (such as a mouse) or Imaging Devices. The device types and storage types available for selection are built into SafeGuard PortProtector and are found in the *General* tab of the *Device Control* window and the *Storage Control* window described above.
  A device type may be **blocked** (default), **allowed** or **restricted**. If you **restrict** a device type, all devices of this type are blocked unless specifically approved. Storage devices may also have **read only** permissions.
- **Approved Models:** This option refers to approving models of devices or storage devices, such as all HP printers or all M-Systems disk-on-keys.
- **Approved Distinct Devices:** This option refers to approving distinct devices or storage devices, each with its own unique serial number, meaning each is an actual specific device. For example, if you wish to approve the use of the CEO's disk-on-key and block all other disk-on-key devices, you should set the Removable Media storage type to **Restrict**, and then enter the identifying parameters of the CEO's USB in a specific distinct device group.

This section describes how to add approved models or distinct devices, either from the list of devices whose usage was detected in your organization by SafeGuard PortAuditor using the **Add Approved Device** wizard (see *Adding a Device Using the Wizard*), or manually.

You can set permissions for approved models and distinct devices in the *White List* tab of the *Device Control* window and the *Storage Control* window which are divided into the **Approved Models** and **Distinct Devices** sections, as described previously.

- The process of adding approved devices to the white list consists of the following steps:
- Adding a device group
- Adding models and distinct devices to the device group, either via the wizard or manually
- Setting group permissions
- Adding additional group settings (such as log and alert settings)
- Saving the policy

3.4.1 Adding Device Groups

Approved models and distinct devices are arranged in groups so as to make it easier for you to manage related, same-permission devices (for instance all the devices used by the marketing group). Before adding devices you must specify device groups. You may define groups of models or distinct devices, depending on your needs.

To add a new group:

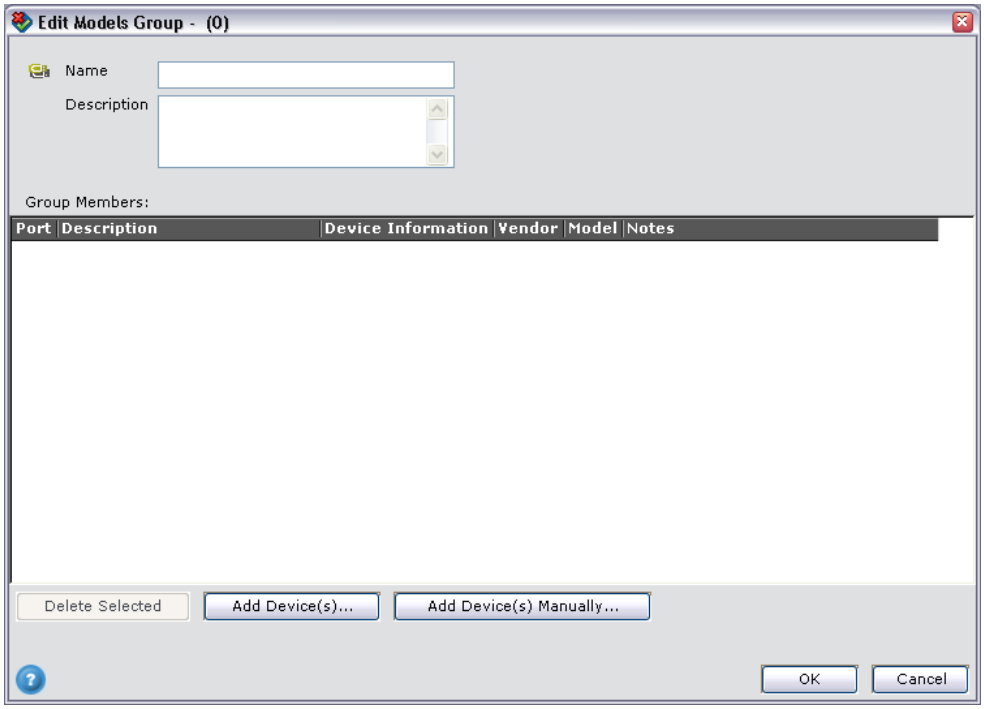
Note: In the **Storage Control** *White List* tab, the lower section is named **Approved Distinct Devices/Media.**

In the Approved Models or Approved Distinct Devices area, click the **New** button

OR

1 Right-click in the **Approved Models** or **Approved Distinct Devices/Media** section of the *White List* tab. A menu opens. If you are in the **Approved Distinct Devices/Media** section of the **Storage Control** *White List* tab, a sub-menu opens.

2 In the menu, click **New Group**. *The Edit Models Group* window opens:



3.4.1.1 Adding a Group

For each device that you have added, the window displays a Description of the device, the device's Vendor, the device Model, the device Distinct ID (in the case of an Approved Distinct Devices group and Notes, if they exist).

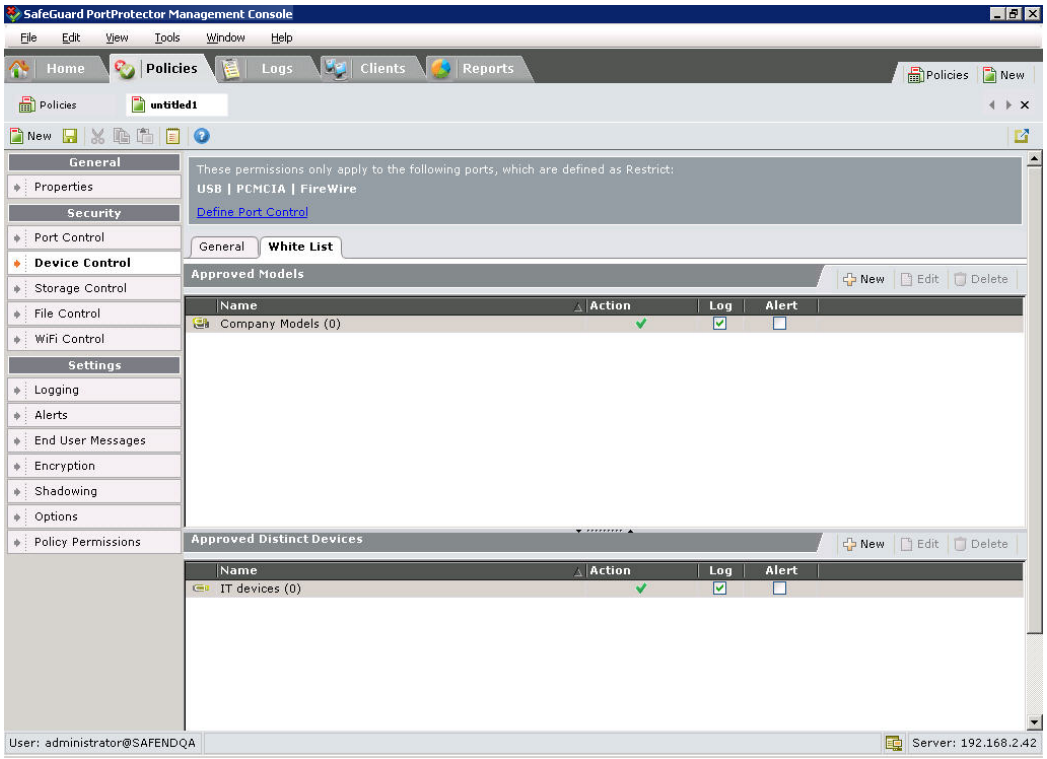
1 The buttons below the device list enable you to delete devices, or add devices, either using the Add Approved Device Wizard (see *Adding a Device Using the Wizard*) or manually (see *Adding a Device Manually*). Alternatively, you can right-click the blank area below **Group Members and select** and select **Add Device Wizard** or **Add Device Manually.**
In this window, enter the desired group **Name** (required) and **Description** (optional)

2 Add devices to the group as described below. You can also add devices to this group at a later time.

3 When you are done, click **OK**.

You may also **Paste** a group from the clipboard by using the **Paste** toolbar button or the **Paste** option in the *Edit* menu.

Once a group has been added, you can see it in the *White List* tab, as follows:



In the figure above, you can see the *Company Models* group. The group is automatically marked as allowed (✔).

3.4.2 Editing a Device Group

Once a group has been created, it may be modified.

To edit a device group:

In the *White List* tab, double-click the desired group

OR

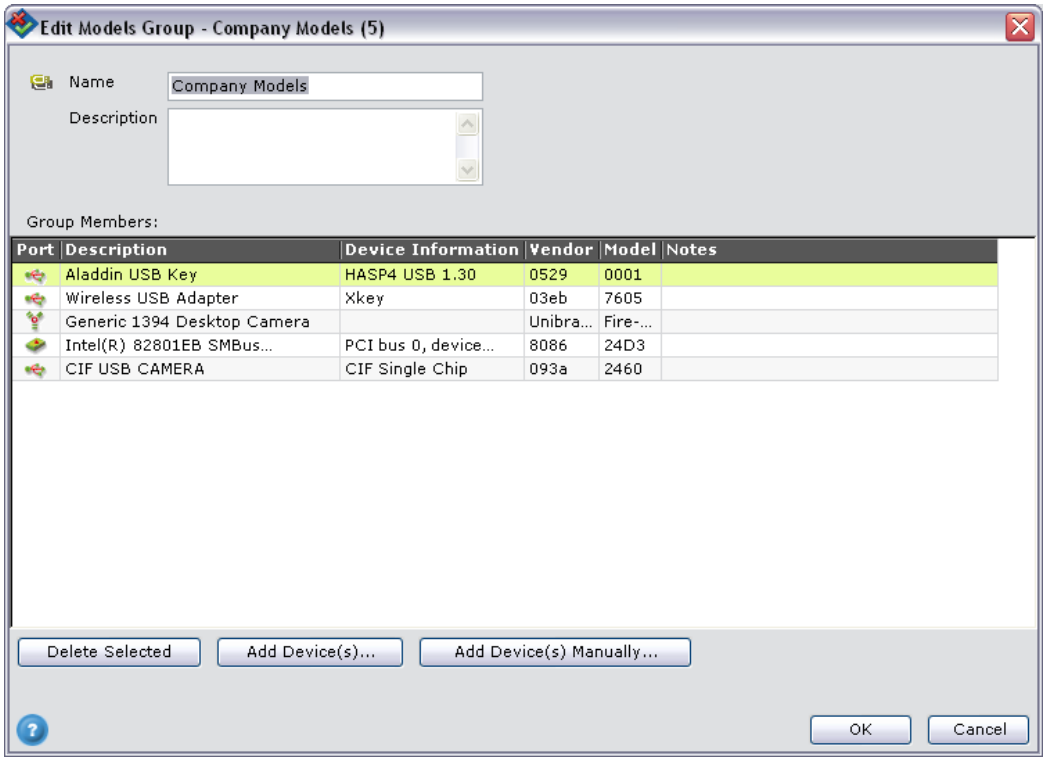
1 Select the group you wish to edit.

2 Click the **Edit Group** button ( ).

OR

Right-click the desired group, then click **Edit** from the menu.

The *Edit Models Group* window opens:



3.4.2.1 Editing a Group

If you have already added devices to this group, the window displays the devices that belong to the group. For each device it displays a Description of the device, the device's Vendor, the device Model, the device Distinct ID (in the case of an Approved Distinct Devices group and Notes, if they exist).

The buttons below the device list enable you to delete devices, or add devices, either using the Add Approved Device Wizard (see *Adding a Device Using the Wizard*) or manually (see *Adding a Device Manually*).

The following edit options are available:

- Adding devices
- Modifying device information
- Deleting devices
- Copying devices to another group or pasting from another group
- Modifying group **Name** and **Description**

3.4.3 Adding Devices

Devices can be added to existing device groups, or to a new group as part of the process of adding the group.

To add a device to an existing group:

Right-click the desired group and select **Add to Group.** To add a device using the **Add Approved Device** wizard**,** click **Add via Wizard** and continue according to the instructions in *Adding a Device Using the Wizard*. To add a device manually, click **Add Manually** and continue according to the instructions in *Adding a Device Manually*.

Another way to add a device to an existing group is in the *Edit Group* window, as follows:

1 Open the Edit Group window in one of the ways explained in *Editing a Device Group*.

2 To add a device using the **Add Approved Device** wizard**,** click **Add Devices**(**s**) and continue to the next section – *Adding a Device Using the Wizard*.
To add a device manually, click **Add Device**(**s**) **Manually** and continue to *Adding a Device Manually*.
Additionally, if you have copied USB device information from a log (see *Copying Record USB Device or CD/DVD Medium Information* in *Chapter 5, Viewing Logs*), you can right-click in the blank area of the *Edit Group* window and select **Paste** to copy the USB device information into a group (make sure you are not copying storage device information into a non-storage group or vice versa).

You can use the same steps to add devices while opening a new group.

Note: When you add a device that already belongs to another device group in this policy, and the groups' permissions differ, the most permissive will apply: **Allow** is the most permissive, **Encrypt** is less permissive (it is the same as **Allowed** when encrypted) and **Read Only** is the least permissive.

For example, if the Approved Models group that contains a storage device is set to **Allow**, and the distinct device is set to **Read Only**, the **Allow** permission will apply. Log and Alert settings will also be taken from the most permissive definition.

In cases where a device belongs to more than one group, and those groups have the same permissions, SafeGuard PortProtector will choose between the groups arbitrarily. If the groups do not have the same log and alert settings, it cannot be predicted which settings will apply.

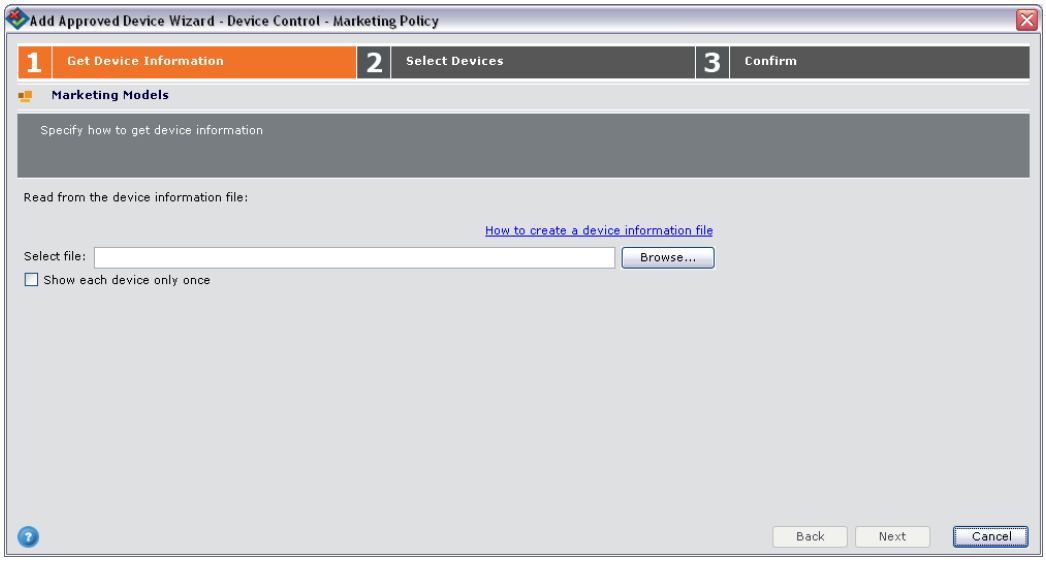
3.4.4 Adding a Device Using the Wizard

Once you have defined device groups, a simple **Add Approved Device** wizard is provided to walk you through the stages of adding approved devices from a list of the devices previously detected on the computers in your network by SafeGuard PortAuditor. You can also add devices manually, as explained in *Adding a Device Manually*. The wizard opens when you click **Add Device(s)** in the *Edit Group* window or when you select **Add via Wizard** from the right-click menu, as explained in *Adding Devices*.

The wizard comprises three steps:

- Step 1: Get Device Information
- Step 2: Select Devices
- Step 3: Confirm

3.4.4.1 Step 1: Get Device Information



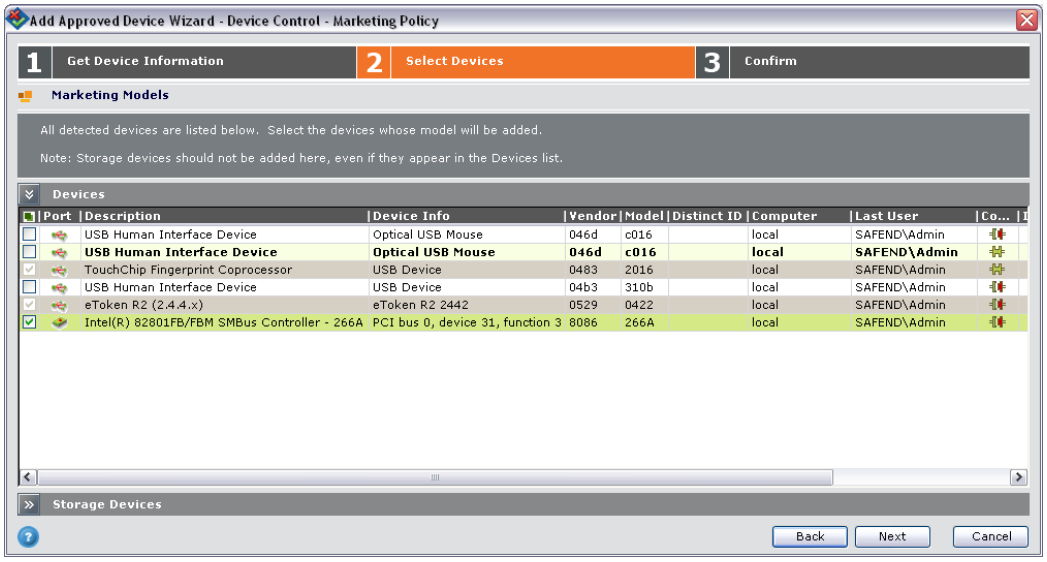
3.4.4.1.1 Getting Device Information

This step enables you to specify the file from which to gather the information about devices that will be added to the group, meaning the location of the SafeGuard PortAuditor .XML file that contains the required device information. Once you select the desired file using **Browse**, click **Next** to continue to step 2.

3.4.4.1.1.1 Creating a Device Information File

In order to create a file that contains the information about the devices you wish to approve, use SafeGuard PortAuditor to scan the required computers. SafeGuard PortAuditor scans the selected computers and reports on all devices and WiFi networks currently or previously connected to those computers. The audit results are stored in a .XML file. To learn about SafeGuard PortAuditor refer to *SafeGuard PortAuditor 3.2 User Guide*.

3.4.4.2 Step 2: Select Devices


Add Approved Device Wizard - Device Control - Marketing Policy
1 Get Device Information
2 Select Devices
3 Confirm
Marketing Models
All detected devices are listed below. Select the devices whose model will be added.
Note: Storage devices should not be added here, even if they appear in the Devices list.
Devices
Port | Description | Device Info | Vendor | Model | Distinct ID | Computer | Last User | Co... |
USB Human Interface Device | Optical USB Mouse | 046d | c016 | local | SAFEND\Admin
USB Human Interface Device | Optical USB Mouse | 046d | c016 | local | SAFEND\Admin
TouchChip Fingerprint Coprocessor | USB Device | 0483 | 2016 | local | SAFEND\Admin
USB Human Interface Device | USB Device | 04b3 | 310b | local | SAFEND\Admin
eToken R2 (2.4.4.x) | eToken R2 2442 | 0529 | 0422 | local | SAFEND\Admin
Intel(R) 82801FB/FBM SMBus Controller - 266A | PCI bus 0, device 31, function 3 | 8086 | 266A | local | SAFEND\Admin
Storage Devices
Back
Next
Cancel

3.4.4.2.1 Selecting Devices

Step 2 displays a table of the devices detected on the endpoints in your network and enables you to select which of these to add to the device group. The table is divided into categories, depending on whether the group to which you are adding devices is an Approved Models group or a Distinct Devices group, and whether you are adding storage devices or non-storage devices.

Selectable devices have a checkbox beside them which you should check if you want to approve the device model or the distinct device, as the case may be. Devices that already belong to the current group are highlighted in gray, and the checkbox beside them is checked.

Note: You cannot add storage devices to the *Device Control* white list.

Note: You cannot add devices or storage devices without a distinct ID to a Distinct Devices group.

Occasionally, a device may not be identified as a storage device by SafeGuard PortAuditor. This may happen, for example, when a device class has not been embedded by the manufacturer. In this case, if you know that it is in fact storage, you may add it to your policy's storage white list.

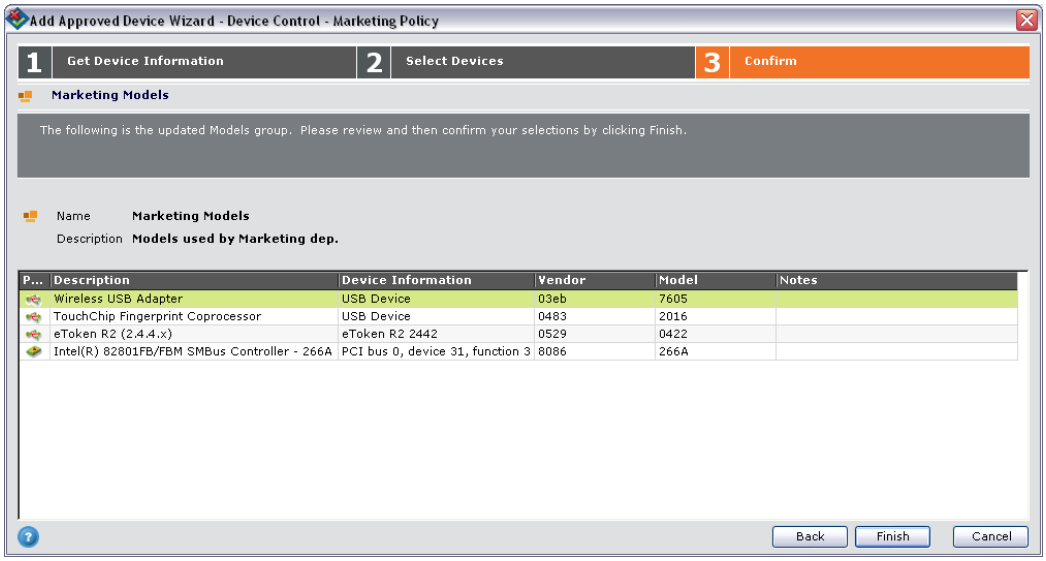
You must avoid adding storage devices to a *Device Control* white list or adding non-storage devices to a *Storage Control* white list, as they will be ignored by the SafeGuard PortProtector Client.

Note: When you add a device that already belongs to another device group in this policy, and the groups' permissions differ, the most permissive will apply. For example, if the Approved Models group that contains a storage device is set to **Allowed**, and the distinct device is set to **Read Only**, the **Allowed** permission will apply. Log and Alert settings will also be taken from the most permissive definition.

In cases where a device belongs to more than one group, and those groups have the same permissions, SafeGuard PortProtector will choose between the groups arbitrarily. If the groups do not have the same log and alert settings, it cannot be predicted which settings will apply.

Once you have selected the devices you want to add to the group click **Next** to continue to step 3.

3.4.4.3 Step 3: Confirm


Add Approved Device Wizard - Device Control - Marketing Policy
1 Get Device Information
2 Select Devices
3 Confirm
Marketing Models
The following is the updated Models group. Please review and then confirm your selections by clicking Finish.
Name Marketing Models
Description Models used by Marketing dep.
P... Description Device Information Vendor Model Notes
Wireless USB Adapter USB Device 03eb 7605
TouchChip Fingerprint Coprocessor USB Device 0483 2016
eToken R2 (2.4.4.x) eToken R2 2442 0529 0422
Intel(R) 82801FB/FBM SMBus Controller - 266A PCI bus 0, device 31, function 3 8086 266A
Back
Finish
Cancel

3.4.4.3.1 Confirming Selection

This is where you confirm your selection and review the group with its newly added devices.

To confirm your selection, click **Finish**, or click **Back** to return to the previous stage.

3.4.5 Adding a Device Manually

You may want to add devices manually (not via the Add Approved Device wizard), as in the case of devices that have not been connected to any endpoint in your organization and therefore do not appear in the SafeGuard PortAuditor audit results. Depending on whether you are adding an Approved Model or a Distinct Device, the *Add Device Model* or *Add Distinct Device* window opens when you click **Add Device(s) Manually** in the *Edit Group* window or when you select **Add Manually** from the right-click menu described in Adding Devices above.

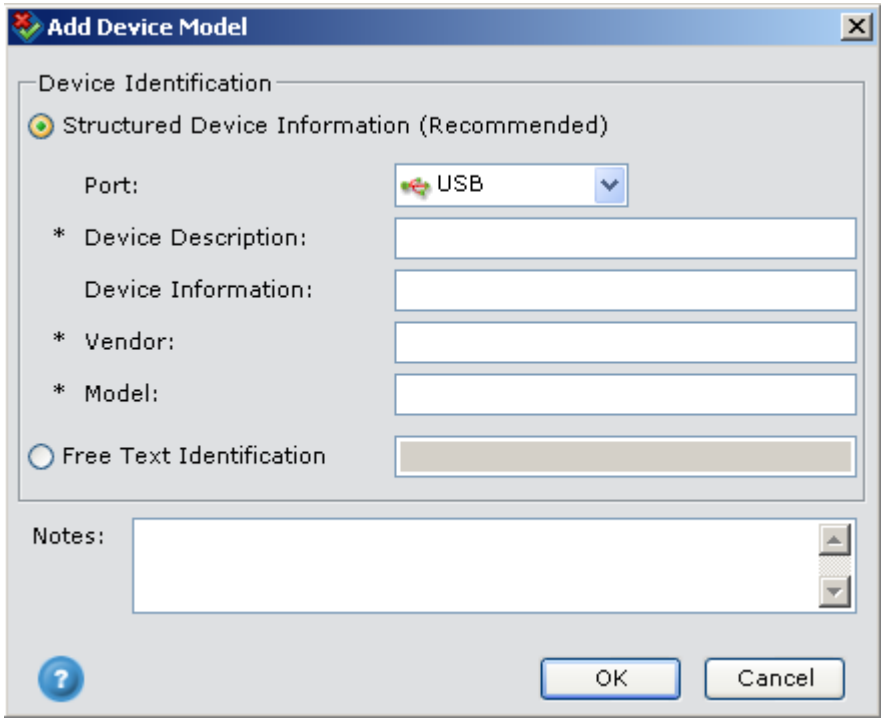
The instructions that follow apply both when adding storage devices (in *Storage Control*) and when adding non-storage devices (in *Device Control*).

Note: When you add a device that already belongs to another device group in this policy, and the groups' permissions differ, the most permissive will apply. For example, if the Approved Models group that contains a storage device is set to **Allowed**, and the distinct device is set to **Read Only**, the **Allowed** permission will apply. Log and Alert settings will also be taken from the most permissive definition.

In cases where a device belongs to more than one group, and those groups have the same permissions, SafeGuard PortProtector will choose between the groups arbitrarily. If the groups do not have the same log and alert settings, it cannot be predicted which settings will apply.

3.4.5.1 Adding an Approved Model

When you add a device model to an Approved Models group, the *Add Device Model* window opens:



Two options are provided for identifying the device:

- **Structured Device Information:** which enables you to fill in fields that specify the informaton on the device that enables SafeGuard PortProtector to identify it, as described in the next section below. This is the recommended option. It is appropriate for the majority of devices, because it is based on common device information conventions that are used by most hardware vendors.
- **Free Text Identification:** which enables you to enter free text to specify the informaton on the device that enables SafeGuard PortProtector to identify it. Only use this option if you cannot see the fields provided in the **Structured Device Information** option in the SafeGuard PortProtector logs.

3.4.5.1.1 Entering Device Model Information

In the *Add Device Model* window, enter the device model information as described below:

To add a device model:

1 Select the device identification method: Structured Information (recommended) or Free text Identification, as described above

2 If you have chosen structured device identification:

- In the **Port** menu, select the port type.

Note: More than one option is available for FireWire and PCMCIA ports. If you are uncertain which is the correct option for the port, check the Windows Device Manager or SafeGuard PortAuditor scan results.

3 Enter the required information in the following fields:

- Device Description – required.
- Device Information – optional.
- Vendor (Vendor ID) – required.
- Model (Product ID) – required.

Note: Vendor ID (VID) and Product ID (PID) can be found in SafeGuard PortAuditor scan results, on a sticker attached to the product itself or in Windows Device Manager

Only use **Free Text Identification** option when the Vendor and Model fields are empty in the logs generated by the device you wish to white list. In the **Free Text Identification** field, you can enter your device's Hardware ID.

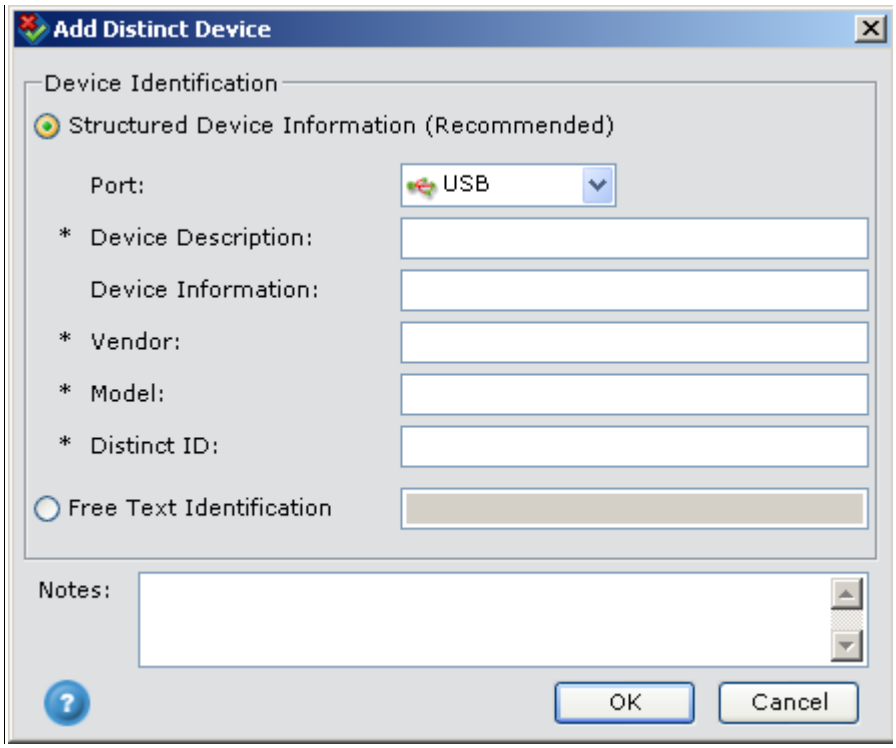
Note: Hardware ID can be found in the **Device Manager** - **Details** tab.

4 Enter **Notes** – optional

5 Double-check that you have entered the correct data in all the fields and click **OK**.

3.4.5.2 Adding a Distinct Device

When you add a device to an Approved Models group, the *Add Distinct Device* window opens:



The window differs from the *Add Device Model* window in that it includes an additional, required field – **Distinct ID**.

3.4.5.2.1 Entering Distinct Device Information

In the *Add Distinct Device* window, enter the device model information as described below:

To add a distinct device:

1 Select the device identification method: Structured Information (recommended) or Free text Identification, as described above

2 If you have chosen structured device identification:

- In the **Port** menu, select the port type.

Note: More than one option is available for FireWire and PCMCIA ports. If you are uncertain which is the correct option for the port, check the Windows Device Manager or SafeGuard PortAuditor scan results.

- Enter the required information in the following fields:
- Device Description – required.
- Device Information – optional.
- Vendor (Vendor ID) – required.
- Model (Product ID) – required.

Note: Vendor ID (VID) and Product ID (PID) can be found in SafeGuard PortAuditor scan results, on a sticker attached to the product itself or in Windows Device Manager.

Only use **Free Text Identification** option when the Vendor and Model fields are empty in the logs generated by the device you wish to white list. In the **Free Text Identification** field, you can enter your device's Hardware ID.

Note: Hardware ID can be found in the **Device Manager** - **Details** tab.

3.4.6 Additional Device Group Settings

Once you have added the desired devices to a group, you need to define a few more settings:

- Log and alert settings
- Action (storage devices only)
- Group permissions, specifically Disk-on-key Smart Functionality settings (storage devices only)

To define log and alert settings:

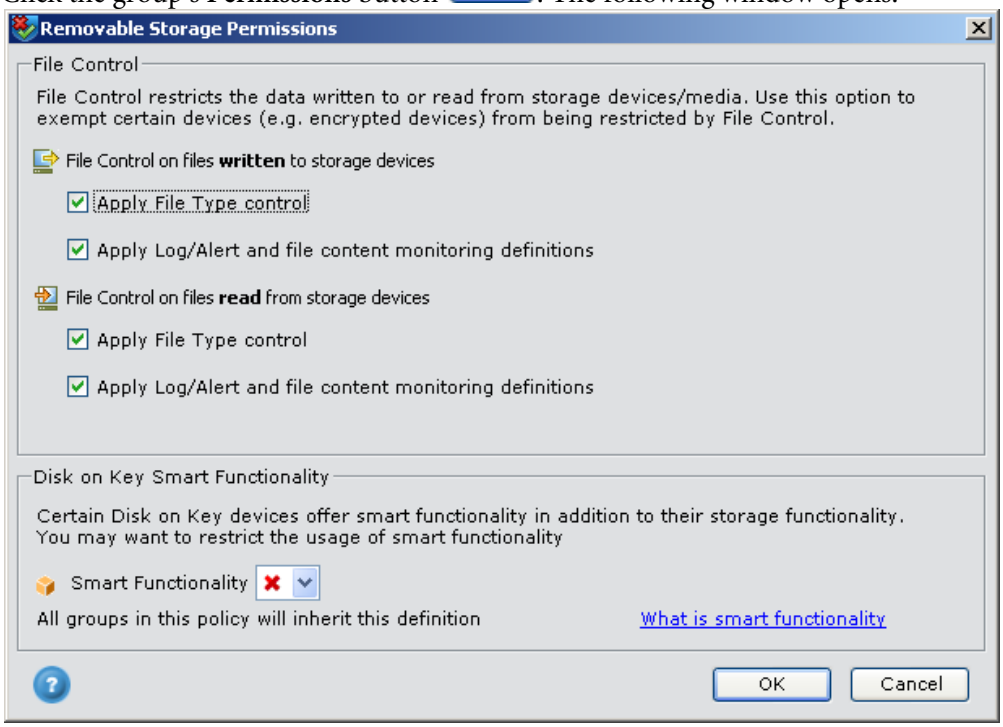
For each group, check the *Log* and *Alert* checkboxes as required.

To set group definitions (storage only):

In the group's *Action* menu, select whether the group's permissions is **Allow** ( ), **Encrypt** ( ) or **Read Only** ( ) (non-storage devices are set to **Allowed** automatically and cannot be configured).

To define disk-on-key Smart Functionality settings (storage only):

Click the group's **Permissions** button ... . The following window opens:


Removable Storage Permissions
File Control
File Control restricts the data written to or read from storage devices/media. Use this option to exempt certain devices (e.g. encrypted devices) from being restricted by File Control.
File Control on files written to storage devices
Apply File Type control
Apply Log/Alert and file content monitoring definitions
File Control on files read from storage devices
Apply File Type control
Apply Log/Alert and file content monitoring definitions
Disk on Key Smart Functionality
Certain Disk on Key devices offer smart functionality in addition to their storage functionality. You may want to restrict the usage of smart functionality
Smart Functionality
All groups in this policy will inherit this definition
What is smart functionality
OK
Cancel

3.4.6.1 Storage Group Permissions

If you wish, you may set group-specific definitions for Disk On Key smart functionality. These definitions will override the smart functionality definitions you set in the *General* tab.

Click the first radio button if you want to use the definitions you have defined in the *Storage Devices - General* tab.

If you want to set specific definitions for the devices in this group, click the second radio button, then select the required permission from the **Smart Functionality** drop-down menu (refer to *Setting Removable Storage Permissions* for an explanation of smart functionality).

3.4.7 Adding WiFi Connections

WiFi links are added to the *WiFi Control* white list in much the same way this is done in the case of devices; adding WiFi groups, then adding approved links to these groups using the **Add Approved WiFi** wizard, or manually.

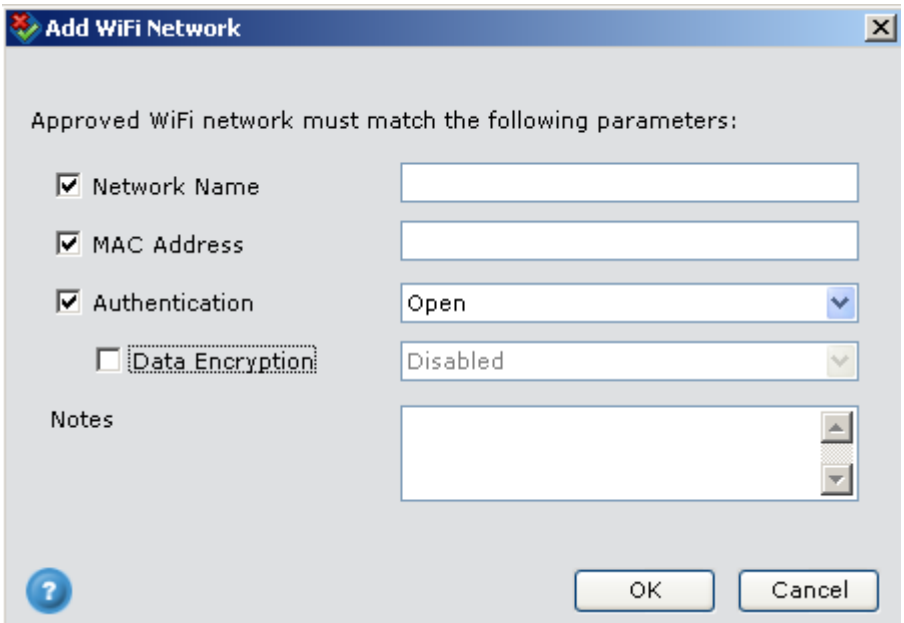
To add approved WiFi links:

With the exception of adding WiFi links manually, simply follow the instructions provided for adding devices, as follows:

- *Adding Device Groups*
- *Adding Devices*
- *Adding a Device Using the Wizard*
- *Additional Device Group Settings*

3.4.7.1 Adding a WiFi Link Manually

When you want to add WiFi links that were not detected by SafeGuard PortAuditor, and as a result cannot be added using the wizard, you can do so manually. When you select to add a network manually, the following window opens:



3.4.7.1.1 Entering WiFi Network Information

In this window you define the parameters a network must match in order for it to be approved for connection. You can identify a network by one or more of the following: its name, its MAC address or its authentication type. After you enter a network authentication type, you can also specify data encryption parameters which must be matched. Only networks matching all the parameters are approved.

In the *Add WiFi Network* window, enter the network information as described below:

To add a WiFi link manually:

1 In the *Add WiFi Network* window, check one or more of the following: **Network Name**, **MAC Address** or **Authentication**.

2 If you have checked **Network Name** , enter the name and continue.

3 If you have checked **MAC Address**, enter the address and continue.

4 If you have checked **Authentication**, you may choose the authentication type from the menu. You might want to define the **Data Encryption** also.

Note: The **Data Encryption** options available in the menu depend on the selected **Authentication** type. For example, for WPA authentication, the encryption options are TKIP or AES, whereas in the case of 802.1X authentication only WEP encryption is available for selection.

5 Add **Notes** (optional).

6 Double-check that you have entered the correct data in all the fields and click **OK**.

3.4.8 Deleting a Group

If you wish, you can delete a device group or a WiFi group from the white list. Doing so deletes the group and all its members.

To delete a group:

1 In the White List tab, right-click the group you want to delete.

2 From the menu, click **Delete**. A confirmation window opens. Click **Yes** to delete the group.

OR

1 Select the group you wish to delete.

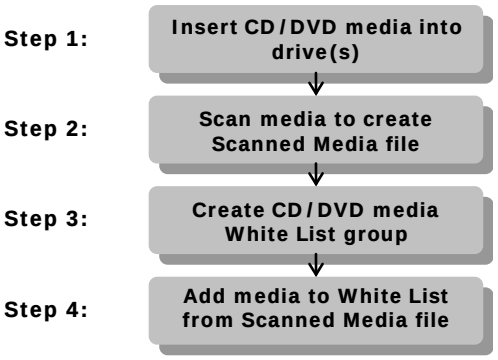
2 Click the **Delete Group** button ( ).

3.5 Approving CD/DVD Media

In addition to controlling CD/DVD drives, SafeGuard PortProtector includes the ability to identify specific CD/DVD media, in order to authorize their use. A special scanning mechanism known as the Media Scanner computes a unique "fingerprint" identifying the data on each medium. Any change made to the data on the medium will revoke its fingerprint, making it unapproved.

With this feature administrators can restrict users to use their CD/DVD drives only with approved media. A white list of approved media is maintained by the administrator and may include software installation CDs, media with approved content and so on. Access to these authorized media will be limited to read-only mode so as to ensure they remain unchanged following authorization.

The process of fingerprinting media and adding them to the CD/DVD Media White List is summarized in the following chart:


Step 1:
Insert CD/DVD media into drive(s)
Step 2:
Scan media to create Scanned Media file
Step 3:
Create CD/DVD media White List group
Step 4:
Add media to White List from Scanned Media file

The process of scanning and fingerprinting media and creating a Scanned Media file (steps 1 and 2) is explained in *Appendix D – CD/DVD Media Scanner*. Steps 3 and 4 are described below.

Note: When all CD/DVD Drives are **Allowed**, or when using a CD/DVD drive that is allowed through the White List, all media is **Allowed**. If a white listed, fingerprinted medium is used through an approved CD/DVD device, all actions are allowed on it, including writing. However, if the data on a white listed device is changed, its fingerprint is revoked and it is no longer approved when used through a **Restricted** CD/DVD drive.

This section describes how to add approved CD/DVD media from the Scanned Media file which you created using the Media Scanner (refer to *Appendix D – CD/DVD Media Scanner*) using the **Add Approved Media** wizard (see *Adding a Device Using the Wizard*).

- The process of adding approved media to the white list consists of the following steps:
- Adding a media group
- Adding media to the device group via the wizard
- Adding log and alert settings
- Saving the policy

3.5.1 Adding Media Groups

Similarly to approved models and distinct devices , approved media are arranged in groups so as to make it easier for you to manage related, same-permission media (for instance all the media used by the R&D group); before adding media you must add new media groups.

Note: Prior to adding media groups to the White List you must set CD/DVD Drives to **Restrict** in the Storage Control *General* tab.

To add a new media group:

1 In the Storage Control *White List* tab, in the **Approved Distinct Devices/Media** area, click the **New** button

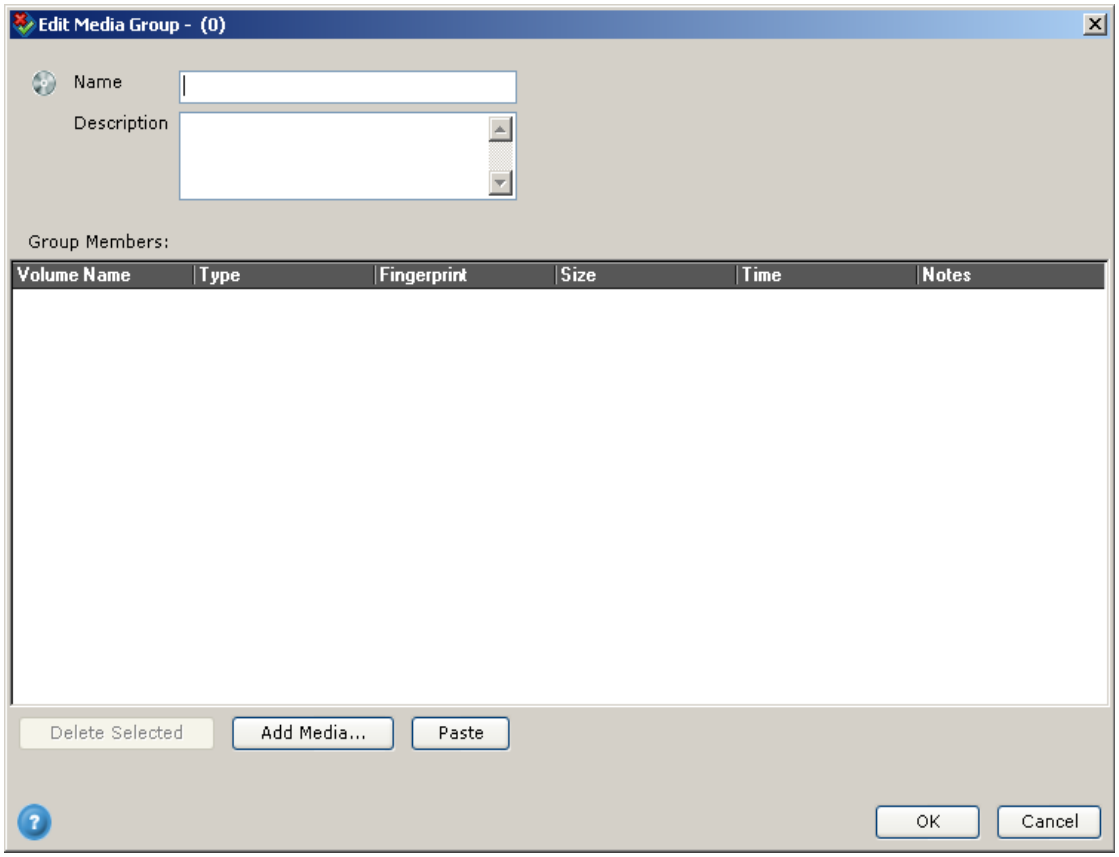
. A menu opens.

2 In the menu, select *Media Group*. The *Edit Media Group* window opens.

OR

1 Right-click in the Approved Distinct Devices/Media section of the White List tab. A menu opens.

2 In the menu, select New Group, and in the sub-menu select Media. The *Edit Media Group* window opens:



3.5.1.1 Adding a Media Group

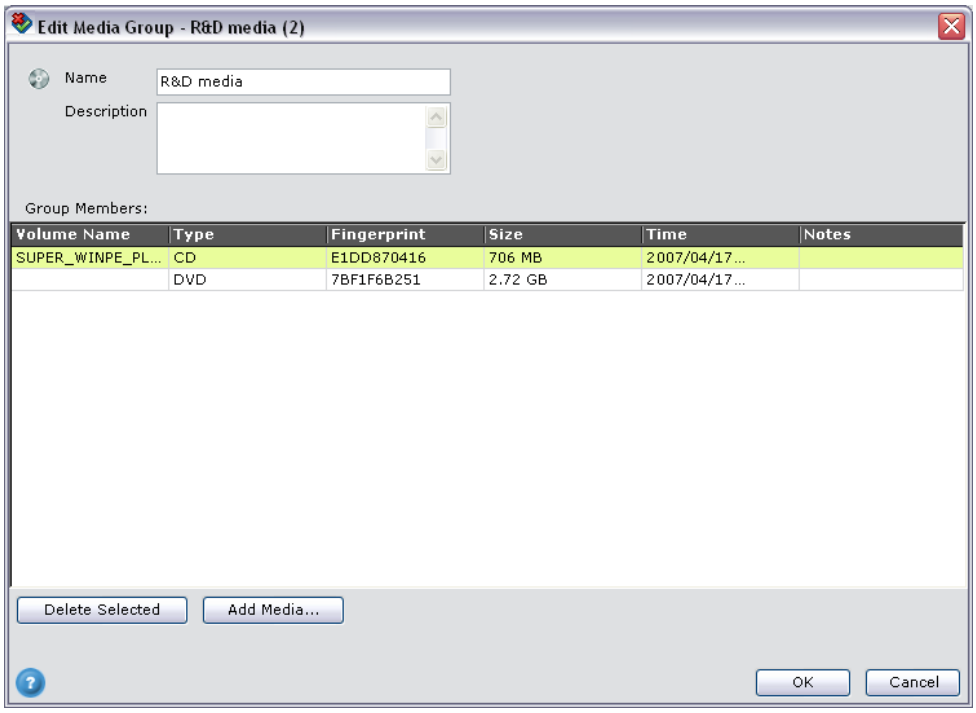
For each medium in this group, the *Edit Media Group* window displays the following information:

- **Volume Name:** name of the scanned volume, if one has been assigned
- **Type:** CD or DVD
- **Fingerprint:** the fingerprint assigned to the medium by the Media Scanner (see *Appendix D – CD/DVD Media Scanner*)
- **Size:** size of the content on the medium
- **Time:** date and time when medium was scanned
- **Notes:** any notes which you have added

To add a CD/DVD media group:

1 The buttons below the device list enable you to delete media, or add media using the **Add Approved Media** Wizard (see *Adding a Device Using the Wizard*). In the window, enter the desired group **Name** (required) and **Description** (optional).

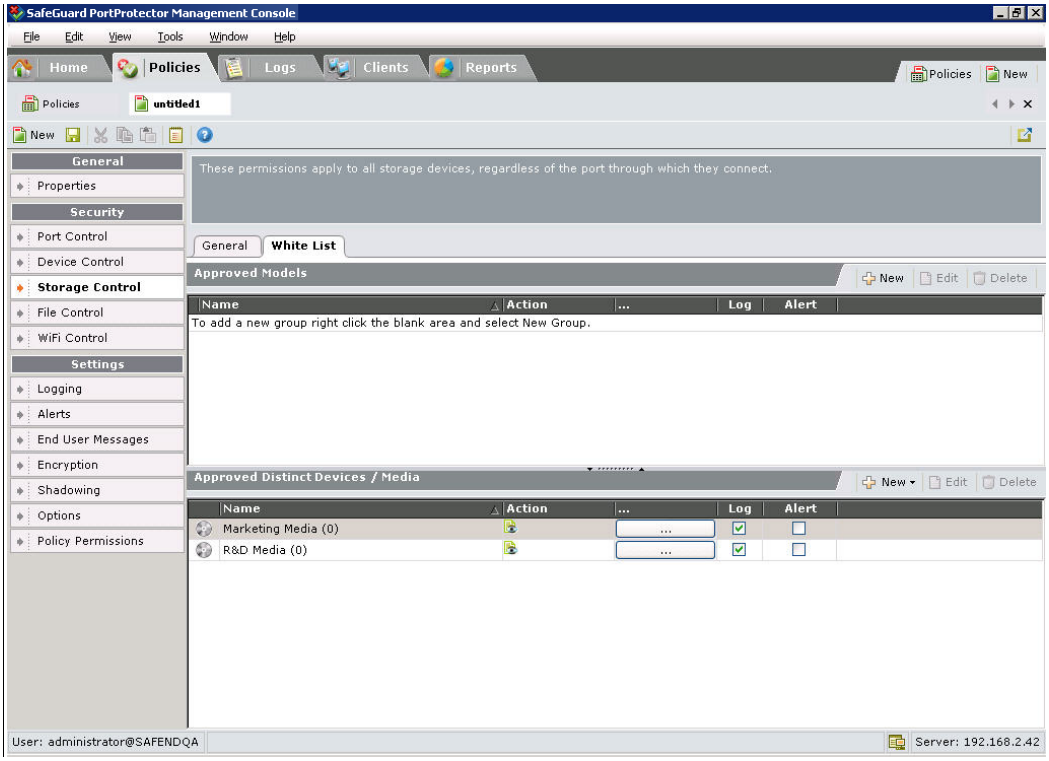
2 Click **Add Media** to add media to the group as described in *Adding a Device Using the Wizard*. Alternatively, right-click the blank area under **Group Members** and select **Add Media**.
You may also add media to this group at a later time. Once you have added media to the group, they appear in the window as follows:



3 When you are done, click **OK**.

You may also **Cut** and **Paste** a group from the clipboard by using the **Cut** and the **Paste** toolbar buttons or *Edit* menu options.

Once a group has been added, you can see it in the *White List* tab, as follows:



In the figure above, you can see two media groups: *Marketing media and R&D media*. The groups are automatically set to Read Only , as approved media contents may not be changed).

3.5.2 Editing a Media Group

Once a group has been created, it may be modified.

To edit a device group:

In the *White List* tab, double-click the desired group

OR

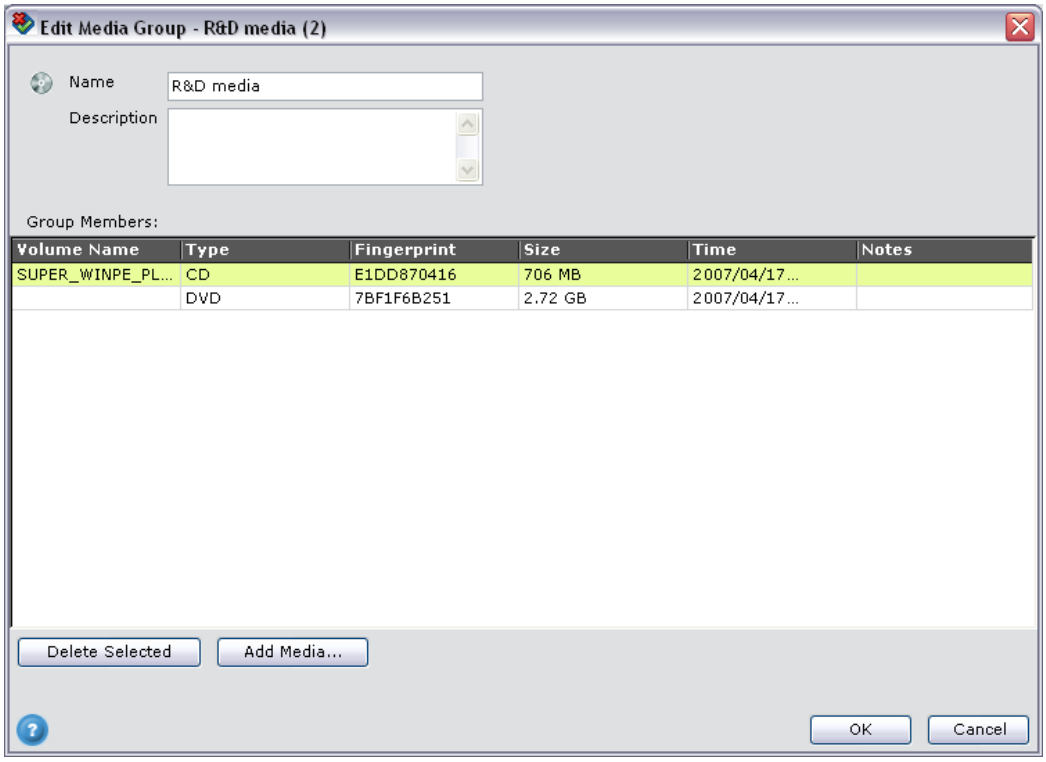
Right-click the desired group, then click **Edit** from the menu.

OR

1 Select the group you wish to delete.

2 Click the **Edit Group** button (Edit).

The *Edit Media Group* window opens:



3.5.2.1 Editing a Group

If you have already added media to this group, the window displays the media that belong to the group. For each medium it displays the following:

- **Volume Name:** name of the scanned volume, if one has been assigned
- **Type:** CD or DVD
- **Fingerprint:** the fingerprint assigned to the medium by the Media Scanner (see *Appendix D – CD/DVD Media Scanner*)
- **Size:** size of the content on the medium
- **Time:** date and time when medium was scanned
- **Notes:** any notes which you have added

The buttons below the list enable you to delete media or add media (see Adding a Device Using the Wizard).

The following edit options are available:

- Adding media
- Modifying medium information
- Deleting media
- Copying media to another group or pasting from another group
- Modifying group **Name** and **Description**

3.5.3 Adding Media

Media can be added to existing groups, or to a new group as part of the process of adding the group.

To add a medium to an existing group:

Right-click the desired group and select **Add to Group.** The **Add Approved Media** wizard opens (see *Adding a Device Using the Wizard)*.

Another way to add a medium to an existing group is in the *Edit Group* window, as follows:

1 Open the Edit Group window in one of the ways explained in Editing a Device Group.

2 Click **Add Media** and continue to the next section – *Adding a Device Using the Wizard*.

Additionally, if you have copied medium information from a log (see *Copying Record USB Device or CD/DVD Medium Information* in *Chapter 5, Viewing Logs*), you can right-click in the blank area of the *Edit Group* window and select **Paste** to copy the medium information into a group (make sure to copy the medium to a Media group and not to a Distinct Device group).

You can use the same steps to add media while opening a new group.

Note: In cases where a medium belongs to more than one group, and those groups have the same permissions, SafeGuard PortProtector will choose between the groups arbitrarily. If the groups do not have the same log and alert settings, it cannot be predicted which settings will apply.

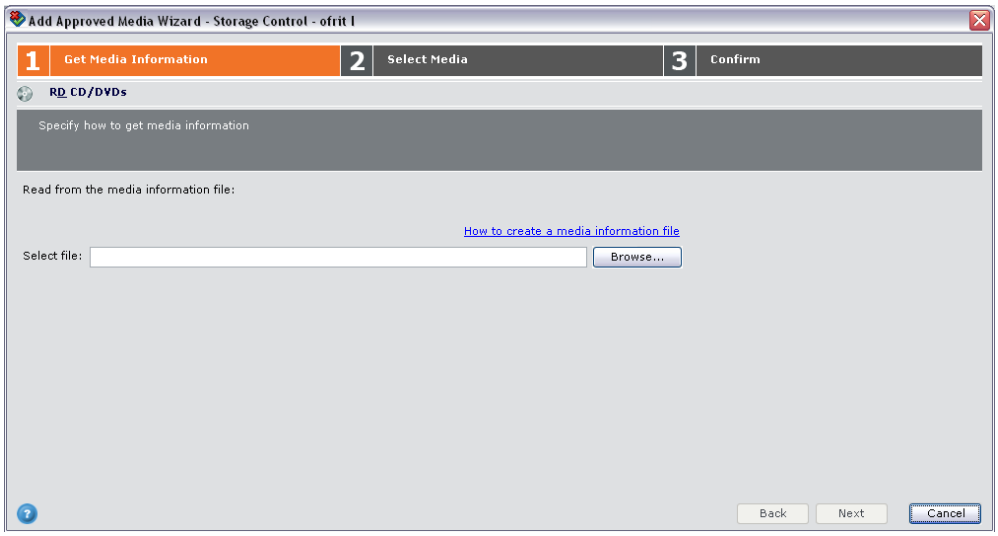
3.5.3.1 Adding a Medium Using the Wizard

Once you have defined a media group, a simple **Add Approved Media** wizard is provided to walk you through the stages of adding approved media from a list of the devices previously scanned by the Media Scanner (refer to *Appendix D – CD/DVD Media Scanner*). The wizard opens when you click **Add Media** in the *Edit Group* window or when you select **Add to Group** from the right-click menu, as explained in *Adding Media*.

The wizard comprises three steps:

- Step 1: Get Media Information
- Step 2: Select Media
- Step 3: Confirm

3.5.3.2 Step 1: Get Media Information



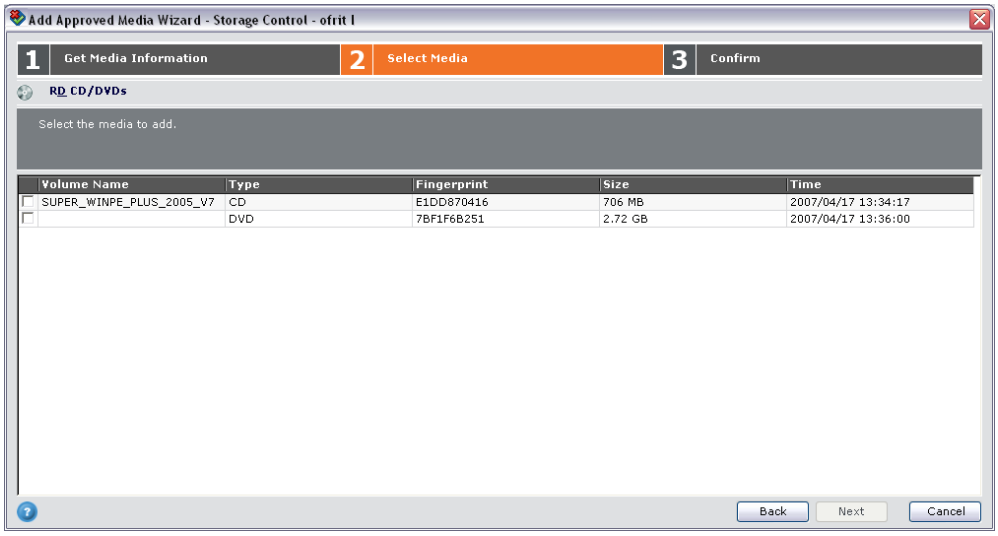
3.5.3.2.1 Getting Media Information

This step enables you to specify the file from which to gather the information about media that will be added to the group, meaning the location of the Media Scanner .XML file that contains the required media information. Once you select the desired file using **Browse**, click **Next** to continue to step 2.

3.5.3.2.1.1 Creating a Media Information File

In order to create a file that contains a list of authorized media and their information (the Scanned Media file), use the Media Scanner. The Media Scanner scans and fingerprints the required media. The scan results are stored in a .XML file. Refer to *Appendix D – CD/DVD Media Scanner* to learn about the Media Scanner.

3.5.3.3 Step 2: Select Media



3.5.3.3.1 Selecting Media

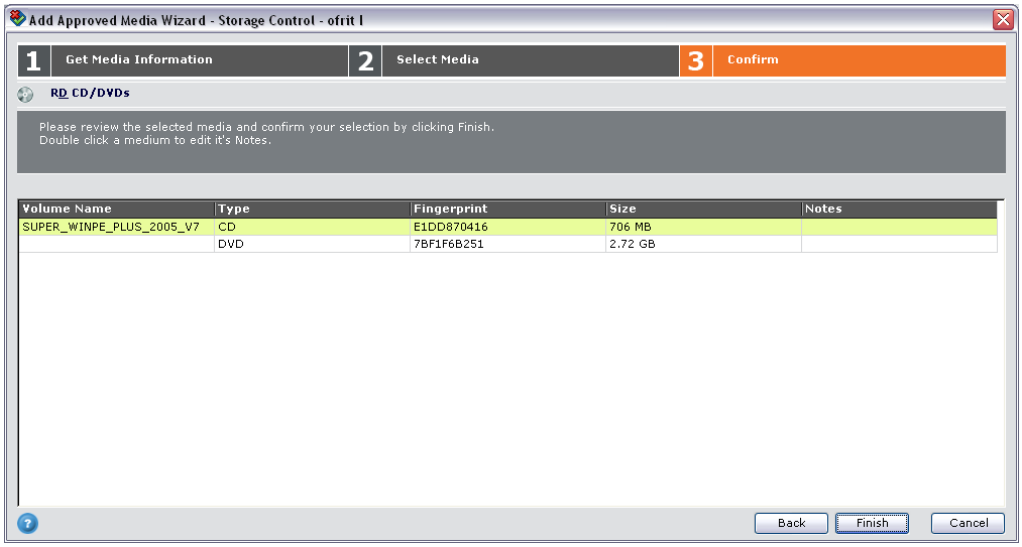
Step 2 displays a table of the media scanned and fingerprinted by the Media Scanner and enables you to select which of these to add to the media group.

Each medium has a checkbox beside it which you should check if you want to approve the medium. Media that already belong to the current group are highlighted in gray, and the checkbox beside them is checked.

Note: In cases where a medium belongs to more than one group, and those groups have the same permissions, SafeGuard PortProtector will choose between the groups arbitrarily. If the groups do not have the same log and alert settings, it cannot be predicted which settings will apply.

Once you have selected the media you want to add to the group click **Next** to continue to step 3.

3.5.3.4 Step 3: Confirm



3.5.3.4.1 Confirming Selection

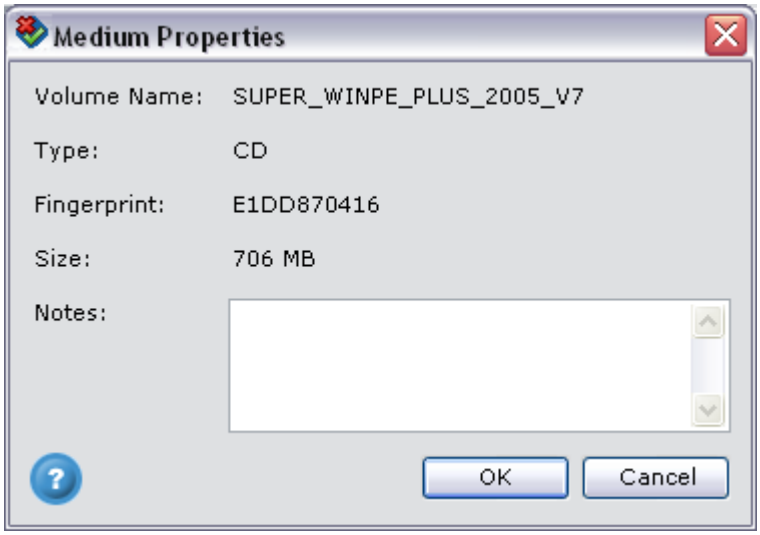
This is where you review the group with its newly added media and confirm your selection. Before confirming, you may add notes to a medium, as explained in *Adding Notes to Medium Properties* below.

To confirm your selection:

1 To add a notes to a medium's properties double-click the medium

OR

Right-click the medium and click **Edit**. The *Medium Properties* window opens:



2 Refer to instructions in *Adding Notes to Medium Properties* below.

3 To confirm your media selection, click **Finish**, or click **Back** to return to the previous stage.

3.5.3.4.1.1 Adding Notes to Medium Properties

In the *Medium Properties* windows, add the desired notes and click **OK**.

3.5.4 Additional Media Group Settings

Once you have added the desired media to a group, you need to define additional settings:

3.5.4.1 Log and Alert Settings

To define log and alert settings:

For each group, check the *Log* and *Alert* checkboxes as required.

Note: The data on approved CD/DVD media may not be changed. Therefore, the **Action** for Approved Media group is always set to Read Only.

3.5.4.2 Media Group Permissions

Approved Media group permissions are not configurable, since File Control does not apply to approved media. This means that once approved, any type of file may be read from these media.

3.6 Managing Policies

The *Policies* window shown below is a central focal point through which you can view a list of your policies and perform various actions such as edit policies, delete policies, export policies and more.

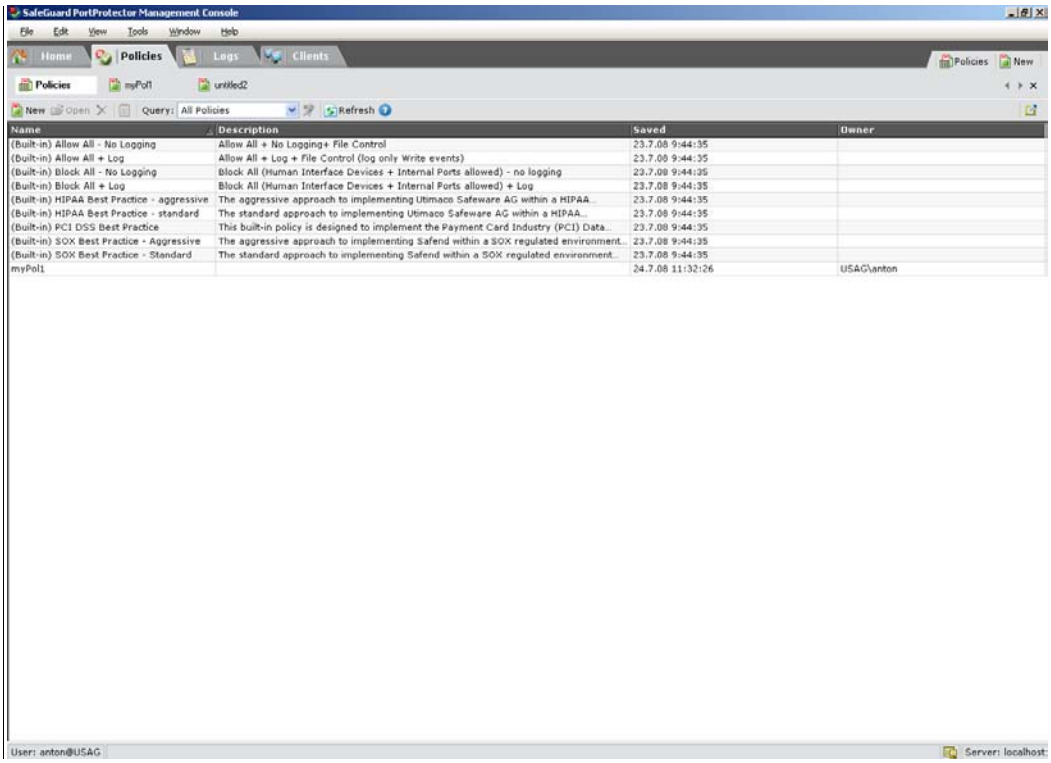
This window is displayed automatically when you initially open the Policies World by clicking the *Policies* tab. After you have switched to other windows in the Policies World, you can return to the *Policies* window by various means, as follows:

To open the Policy Management (*Policies*) window:

From the Window Bar or from the top right-hand corner of the window, click the **Policies** icon ( )

OR

From the File menu, click **Policies**. The *Policies* window opens.


SafeGuard PortProtector Management Console
File Edit View Tools Window Help
Home Policies Logs Clients
Policies New
Policies myPol1 untitled2
New Open Query: All Policies Refresh
Name Description Saved Owner
(Built-in) Allow All - No Logging Allow All + No Logging+ File Control 23.7.08 9:44:35
(Built-in) Allow All + Log Allow All + Log + File Control (log only Write events) 23.7.08 9:44:35
(Built-in) Block All - No Logging Block All (Human Interface Devices + Internal Ports allowed) - no logging 23.7.08 9:44:35
(Built-in) Block All + Log Block All (Human Interface Devices + Internal Ports allowed) + Log 23.7.08 9:44:35
(Built-in) HIPAA Best Practice - aggressive The aggressive approach to implementing Utimaco Safeware AG within a HIPAA... 23.7.08 9:44:35
(Built-in) HIPAA Best Practice - standard The standard approach to implementing Utimaco Safeware AG within a HIPAA... 23.7.08 9:44:35
(Built-in) PCI DSS Best Practice This built-in policy is designed to implement the Payment Card Industry (PCI) Data... 23.7.08 9:44:35
(Built-in) SOX Best Practice - Aggressive The aggressive approach to implementing Safend within a SOX regulated environment... 23.7.08 9:44:35
(Built-in) SOX Best Practice - Standard The standard approach to implementing Safend within a SOX regulated environment... 23.7.08 9:44:35
myPol1 24.7.08 11:32:26 USAG\anton
User: anton@USAG
Server: localhost

SafeGuard PortProtector Management Console comes with several built-in policies. These are described in *Step 3: Create a Policy*.

In the *Policies* window you can perform the following actions:

- Open a policy, explained in *Opening a Policy*.
- Modify a policy, explained in *Modifying a Policy*.
- Create a new policy, explained in Creating a New Policy.
- Delete a policy, explained in *Deleting Policies*.
- View and print policy summary, explained in *Viewing and Printing Policy Summary*.
- Export or import a policy to/from a file, explained in *Exporting and Importing a Policy*.
- Query policies associated with an organizational object, explained in *Querying Associated Policies*.

3.6.1 Opening a Policy

You can open an existing policy through the *Policies* window.

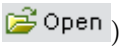
To open a policy:

From the *Policies* window, double-click the policy you wish to open

OR

Right-click the policy and select **Open**.

OR

From the toolbar, click the **Open** button (

).The policy window opens, displaying the policy's definitions.

3.6.2 Modifying a Policy

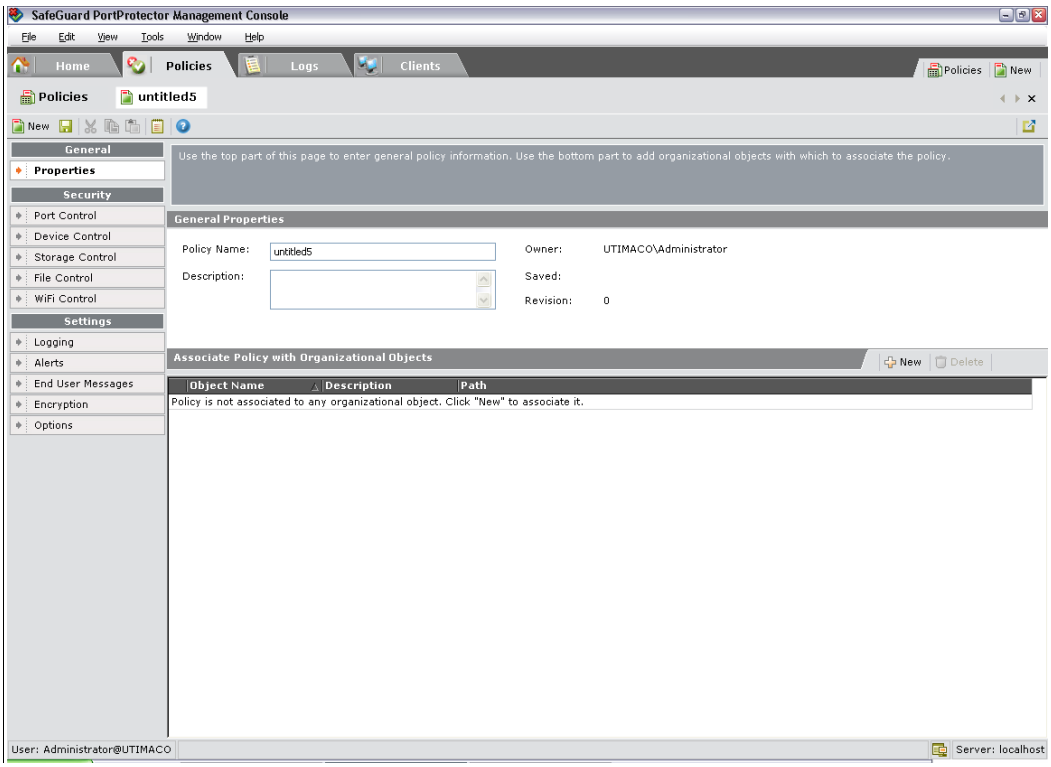
After you have opened a policy, you can modify its definitions and save it, or save it as a new policy under a different name.

3.6.3 Creating a New Policy

Several ways of opening a new default policy are explained in *Step 3: Create a Policy*. Another way to open a new policy is through *Policy Management* window.

To create a new policy from the default settings:

Right-click in the *Policy Management* window and select **New**. An untitled policy opens with default settings. The following window is the initial window that opens:



This window is divided into two sections:

- **General Properties:** the top section. This is where you enter the new policy's name and description (explained below). This section also displays the owner (an administrator) of the policy, the time it was last saved and the revision.
- **Associate Policy with Organizational Objects:** the bottom section. This is where you associate the policy to organizational objects. Refer to *Distributing SafeGuard PortProtector Policies Directly from the* in *Chapter 4, Distributing Policies* for an explanation.

To enter the policy's name and description:

In the general properties section, enter the policy's name and description.

You can now define settings for the policy and save it.

3.6.4 Deleting Policies

You may delete policies that are no longer in use. Deleting policies removes them from Active Directory as well as from the Management Console. You may use the **Ctrl** key to perform a multiple selection of policies to be deleted.

Note: Deleting policies in the Management Console does not remove them from the SafeGuard PortProtector Client on which they are active, and therefore does not compromise your organization's security.

Note: We strongly recommend against deleting policies that are applied on computers and/or users in your organization. Before deleting a policy, keep in mind that once it is deleted you will no longer have any record of the policy definitions. In addition to this, if you ever need to update the policy on Clients protected by the deleted policy, you will have to define a new one.

To delete policies:

In the *Policy Management* window, right-click the policy you wish to delete and select **Delete**

OR

From the toolbar, click the **Delete** button ( ). Following your confirmation, the policy is deleted.

3.6.5 Viewing and Printing Policy Summary

In addition to paging through the various windows in which the policy's settings are defined, you can view the policy's settings in a single-window one-window format which is also suitable for printing.

To view policy summary:

In the *Policy Management* window, right-click the policy you wish to view and select **View Summary**

OR

From the toolbar, click the **View Summary** button ( ).

OR

Select the policy and click **Policy Summary** from the *File* menu.

The *Policy Summary* window opens:

3.6.5.1 Policy Summary

In this window you can view and print policy summary.

To print policy summary:

From the *Summary* window, right-click and select **Print** from the menu.

3.6.6 Exporting and Importing a Policy

You may wish to export policies from the policy database to a file on your computer so that you can use it at a later time (for example, if you want to save the settings you defined in your evaluation copy of the Management Console so that you can use them with your licensed product).Once you have exported the policy, you can import it into the database at a later time.

To export a policy:

In the *Policy Management* window, right-click the policy you wish to export and select **Export**

OR

1 From the *File* menu, click **Export**. The *Export Policy* window opens.

2 Select the desired file name and destination and click **Save.**

To import a policy:

Right-click in the *Policy Management* window and select **Import**

OR

1 From the *File* menu, click **Import**.

2 The *Import Policy* window opens.

3 Select the desired file and click Open. The imported policy opens.

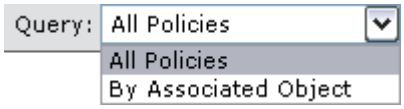
4 To save the policy, use **Save** or **Save As** from the *File* menu.

3.6.7 Querying Associated Policies

If you have used the Policy Server option to associate policies to organizational objects (see *Distributing SafeGuard PortProtector Policies Directly from the* in *Chapter 4, Distributing Policies*), you can query SafeGuard PortProtector Clients in order to learn which policies are associated with a user/computer. With this information, you can figure out what permissions are actually in effect on the user/computer, whether it is associated with one policy or more.

To display policies associated with specified objects:

1 In the *Policies* window, in the *Query* menu shown below that appears in the toolbar, select **By Associated Object** (the other, default option is All Policies).



2 The *Select Object* window opens (this window is discussed in detail in *Associating a Policy to Organizational Objects* in *Chapter 4, Distributing Policies)*.

Note: The *Query* menu appears in the *Policies* window only when the Policy Server option is activated. For details about this option refer to *Distributing SafeGuard PortProtector Policies Directly from the* in *Chapter 4, Distributing Policies*.

3 Filter the *Objects* window as required (as explained in *Selecting and Associating Objects by Name* and *Filtering Objects using the Organizational Tree* in *Chapter 4, Distributing Policies*).

Note: In contrast to filtering objects during Policy Association, when querying associated policies the *Object Type* menu includes only Computers and Users.

4 Click **GO** . The *Objects* window on right hand side now displays a list all the objects that meet the filter criteria.

5 In the list of objects, select the object for which you wish to display associated policies by checking the appropriate checkbox.

Note: Since the purpose of the query is to display policies that are associated with one specific object, only one object may be selected.

6 To display the policies click **OK**. The *Policies* window now displays only the policies associated with the selected object.

To display all policies again:

In the *Policies* window, in the *Query* menu, select All Policies. The *Policies* window now displays all policies.

3.7 Active Window Options

The active policy window can be duplicated, undocked and closed. This is described in *Active Window Options* in *Chapter 2, Getting Started*.

4 Distributing Policies

About This Chapter

This chapter describes how to distribute SafeGuard PortProtector policies to protect the endpoints of your organization.

- *Overview* describes the options for distributing SafeGuard PortProtector policies – directly from the Management Server over SSL (Policy Server), through Active Directory or as registry files (for general use by third-party tools).
- *Distributing SafeGuard PortProtector Policies Directly from the Management Server(s)* describes how to associate policies to organizational objects through the Management Console so that they can be distributed directly from the Server(s) to the SafeGuard PortProtector Clients.
- *Distributing SafeGuard PortProtector Policies Using Active Directory* describes how to assign SafeGuard PortProtector policies (GPOs) to the computers and users in your organization and how to find the required SafeGuard PortProtector policies.
- *Distributing SafeGuard PortProtector Policies Using Registry Files* describes how to store SafeGuard PortProtector policies as registry files in a shared folder in order to use third-party tools to distribute them to the SafeGuard PortProtector Clients. Using this option you can import policies into Novell eDirectory and distribute them using eDirectory capabilities.
- *Policy Merging* describes how SafeGuard PortProtector merges policies when required.

4.1 Overview

SafeGuard PortProtector provides three methods for deploying policies:

- **Directly from the Management Server** (this feature is also named Policy Server): This option enables you to associate policies to organizational objects directly from the Management Console. Following association, policies are distributed from the Management Server directly to SafeGuard PortProtector Clients over SSL.
- **Using Active Directory:** This option uses Active Directory's standard GPO distribution mechanism to distribute policies, as described on the following page. This option is the default. In this case, SafeGuard PortProtector automatically creates (publishes) each policy that you define in SafeGuard PortProtector Management Console as a GPO in Active Directory. These policies are then automatically distributed by Active Directory to the computers and users belonging to the Organizational Unit (OU) to which you assign them.
- **Using Registry Files in a Shared Folder:** This option publishes, or stores, policies as registry files in a shared folder and enables you to update the policy on Clients manually or use third-party tools to publish SafeGuard PortProtector policies to the SafeGuard PortProtector Clients. Refer to Publishing Method in Chapter 7, Administration for more details.

4.2 Distributing SafeGuard PortProtector Policies Directly from the Management Server

One of the main strengths of SafeGuard PortProtector is its deep integration with existing IT infrastructures. Once installed, the product automatically discovers the network, connects to Active Directory (AD) and synchronizes (read-only) with the existing organizational structure, including OU's, Groups, Users and Computers. This process allows the administrator to use his AD objects natively while performing tasks in SafeGuard PortProtector Management Console. Additionally, the system can leverage this highly available and scalable architecture and distribute policies to endpoints via AD's GPO mechanism. However, associating policy objects to users and computers required some user know-how.

An additional method for distributing policies to endpoints is available – the Policy Server. With this feature, policies are distributed directly from the Management Server to the endpoints using the existing SSL infrastructure. To facilitate this, policies are associated to AD or Novell objects from within the Management Console, as a part of the process of defining a policy, with the ability to set policies which are more general (to OU's or Groups) as well as policies which apply to a specific user or computer.

4.2.1 Architecture

If the Policy Server is configured as the conduit for distributing policies, endpoints start to query the Management Server for the policies associated with them. This query is performed each time a computer starts, on user login and at a predefined interval. These communications are very similar to the way logs are sent from endpoints to the server(s), which is web-service based and utilizes SSL for authentication and encryption. There is no need to open any new ports in addition to the ones already used for log collection.

To ensure high performance, scalability and minimal network utilization, multiple optimizations have been added including compression of policies, server side caching and snapshots.

4.2.2 Associating Policies to Organizational Objects

The user interface for defining policies allows for associating a policy to AD/Novell objects. This interface allows the association of a policy to multiple objects of various types. Additional functionality is provided for searching for objects either by name or by navigating the organizational tree.

Policies can be associated to one or more of the following AD/Novell objects:

- Domain
- Organizational Unit (OU)
- Group
- User
- Computer

Note: With the Policy Server, computers that are not managed by AD/Novell (Not in Domain) can also be associated to policies, and can receive policy updates directly from the Management Server.

The Policy Server leverages the policy merging capabilities of the SafeGuard PortProtector Client which allows users to associate multiple policies to one object so that the Client enforces

an aggregated set of permissions from all those policies. Policy merging is described in *Policy Merging*.

4.2.3 Associating a Policy to Organizational Objects

Associating a policy with organizational objects in order to apply the policy to these objects comprises the following steps:

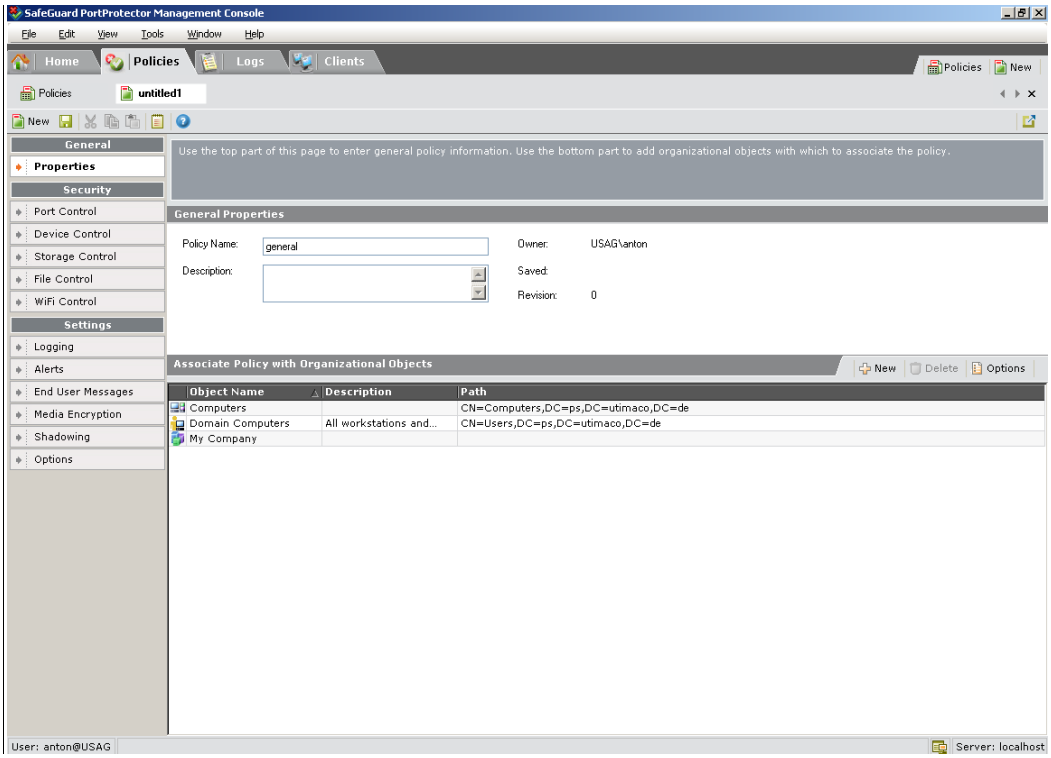
- **Opening the Select Object window**: described in Opening the Select Object Window.
- **Filtering objects and Selecting objects for policy association**: described in *Filtering and Associating Objects*.
- **Restricting the policy to Users/Computers**: described in *Restricting the Policy to Users/Computers*.

Associating a policy to organizational objects is performed from the *Select Object* window which is accessed from the policy's *Properties* tab. The *Select Object* window displays organizational objects from which you select the required one(s). In this window you can filter the organizational units so that the list of objects from which you select the associated objects is focused and meets your needs (for example, if you want to associate a policy to users in a specific domain, there is no need to display other domains or computers in that domain).

Note: Before starting associating you must select Publish policies directly from Server to Clients in the Administration window (see Publishing Method in Chapter 7, Administration)

4.2.3.1 Opening the Select Object Window

The *Select Object* window is opened from the policy's *Properties* tab, shown below:



4.2.3.1.1 Policy Properties Window

This window enables you to enter the policy's name and a description. A new policy contains the default values, or with the policy template values if you have defined such a template (refer to *Policy Template* in *Chapter 7, Administration*).

When you select to publish policies directly from the Management Server to Clients (refer to Publishing Method in *Chapter 7, Administration*), the *Properties* window displays the organizational objects with which this policy is associated. It displays the object name, its description if available and its path. Using the **New** and **Delete** buttons you can add objects to, and delete them from, the list of associated objects. Instructions for selecting objects for association appear in *Selecting an Object for Association* below.

4.2.3.2 Selecting an Object for Association

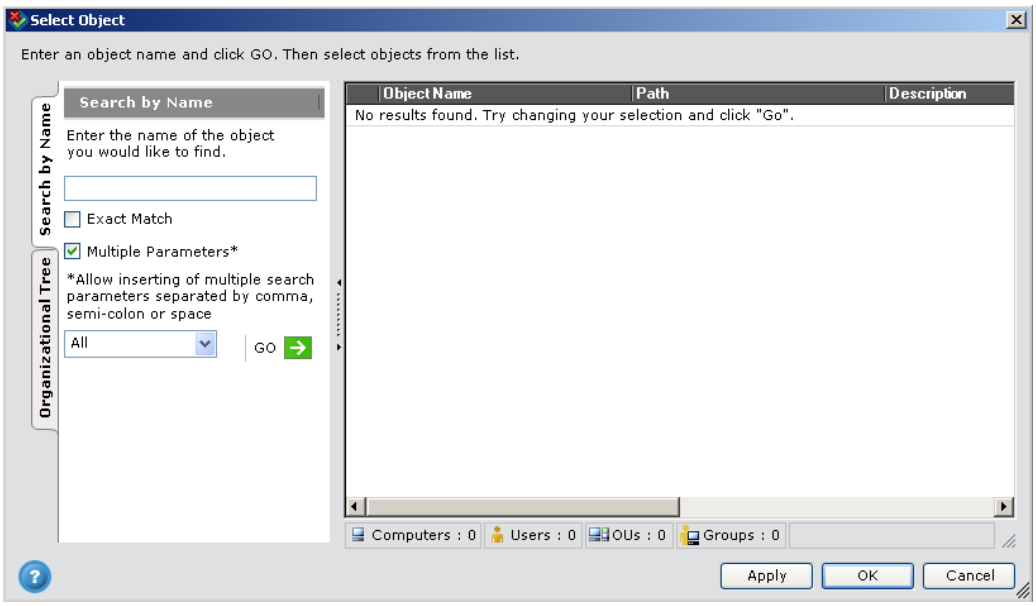
To open the *Select Object* window:

In the bottom section of the policy's *Properties* window (Associate Policy to Organizational Units section), click

OR

Right-click in the bottom section of the window (Associate Policy to Organizational Units).

The *Select Object* window opens:



The Select Object window displays the *Search by Name* and *Organizational Tree* tabs on the left hand side, and the Objects table on the right hand side. The tabs assist you in selecting the required objects with which the policy should be associated. The tabs also contain a drop-down menu (the *Object Type* menu) that enables you to determine which object types should be displayed in the table. The Objects table displays the results of your selection. From the displayed objects you can then select objects to associate.

4.2.3.3 Filtering and Associating Objects

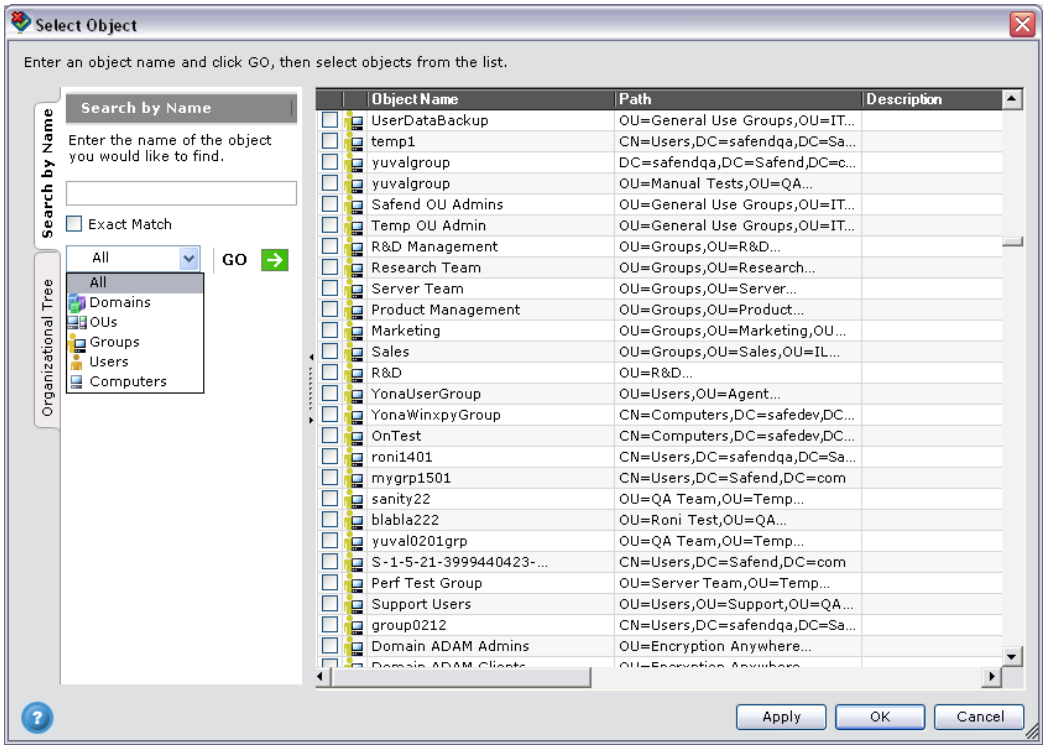
The left-hand side of the *Select Object* window includes two tabs to help you determine the organizational objects that will be displayed in the window and from which you will select the objects with which you wish to associate the policy. These are the *Search by Name* tab and the tab *Organizational Tree*.

Note: If the Domain Partitioning feature is enabled (see *Defining Domain Partitions*), then only the organizational units assigned to this user's role are displayed.

4.2.3.3.1 Filtering Objects by Name

The *Search by Name* tab is a tool that you can use to determine the organizational objects (organizational units, groups, computers, users etc.) to display. The search criteria you enter here determine the objects that will be displayed in the *Objects* table. Once you have selected and displayed those objects, you can then select which of the displayed objects should be associated to the policy.

The following figure displays the *Search by Name* tab:



4.2.3.3.1.1 Selecting and Associating Objects by Name

Note: The instructions in this section also refer to querying associated policies by name. In this case, the result of your selection displays the policies associated with the selected objects in the *Policies* window.

This is where you select objects by their name, and from the displayed list select objects for association.

Note: SafeGuard PortProtector's Domain Partitioning feature enables the partitioning of the Groups, OUs and Domains of an organization so that they are only accessible to the SafeGuard PortProtector Console administrators that are responsible for handling them. Policies that are not associated with all the OUs in an administrator's domain are not displayed and cannot be modified in the **Associate Policy with Organizational Objects** area of the Policy window and in the policy queries.

If however, some of the OUs to which a policy is associated are in an administrator's domain partition (but not others), then this policy may appear in read-only mode.

To search for a specific object:

1 In the text box, enter the name of the computer or user you wish to display. You may enter multiple names separated by comma, semicolon or space.

2 Check the **Exact Match** checkbox if you want to display an object with a name that exactly matches the string you entered in the text box. For computers you must enter the full computer name (including the domain suffix). If **Exact Match** is not selected, the *Select Object* window will display objects whose name contains the string that you entered.

3 From the *Object Type* menu below the search box

, select the object types you wish to display or **All** if you want to display all types.

Note:

When querying associated policies the *Object Type* menu includes only Computers and Users.

4 Click **GO** ( ). The window now displays a table of the objects (one or more) whose name matches your search criteria. If no computer or user is found whose name matches your search criteria, the table is empty and says **No Results Found**.

The Objects table contains a list of the objects that meet your filtering criteria. Each line contains the following columns:

- Checkbox
- Object Name
- Description
- Path

You can modify the table view in the following ways:

- **Sort** the table by clicking the column heading of the column by which you wish to sort. Clicking the header again switch from ascending to descending order. You can add a secondary sort level by pressing the **Shift** key and clicking the secondary column heading.
- **Modify column width** by dragging the column separation lines.
- **Move a column** by dragging and dropping it into the desired position.

To associate a policy with an organizational object:

Note: Instructions 1-3 in this section also refer to querying associated policies by name. In this case, the result of your selection displays the policies associated with the selected objects in the *Policies* window.

1 In the table of objects, select the objects (one or more) to which you wish to associate the policy by checking the appropriate checkboxes.

2 To add the objects to the list of associated objects without closing the window, and to continue adding objects through an additional search, click **Apply**.

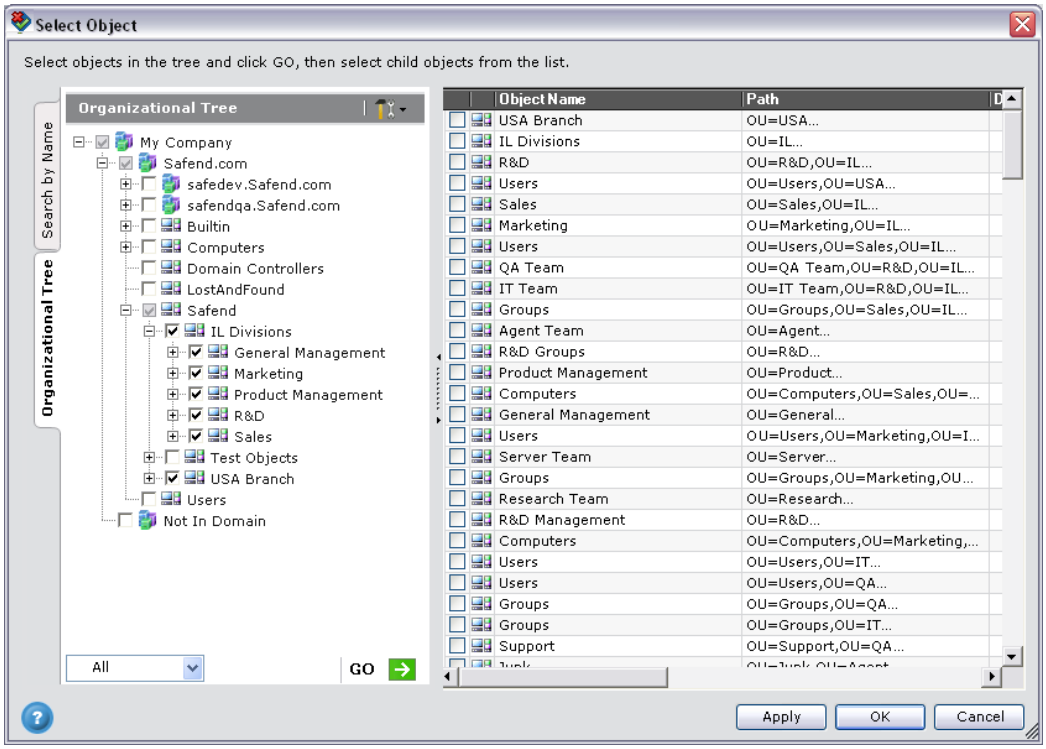
3 To add the objects to the list of associated objects and close the window, click **OK**. The objects are added to the list and the *Select Object* window closes. You can now view a list of the associated objects in the bottom part of the *Properties* window.

4 Save the policy. The policy will be updated on Clients the next time Clients refresh their policy as determined by the interval you set in the policy's Options settings (see *Step 15: Define Options* in *Chapter 3, Defining Policies*).

4.2.3.3.2 Filtering Objects using the Organizational Tree

The Organizational Tree is an additional tool you can use to determine which objects to display in the *Objects* table. Once you have selected and displayed those objects, you can then select which of the displayed objects should be associated to the policy.

The *Organizational Tree* tab displays the domain(s), organizational units, groups, users and computers in your organization, and the Not In Domain group (which includes all computers who do not currently belong to any domain), as shown in the following figure:



Note: The Organizational Tree is applicable only if you are using Active Directory or Novell eDirectory, and if you have set the appropriate Directory definitions in the *Administration* window (refer to *Configuring General Tab Settings* in *Chapter 7, Administration*). If you are not using one of these Directory services, only one group is displayed in the Tree – Not In Domain. Selecting this group selects all computers.

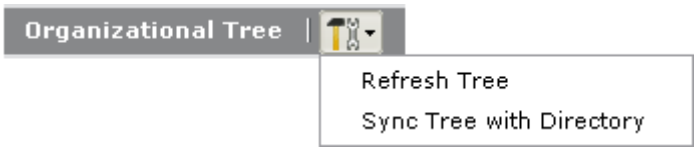
4.2.3.3.2.1 Selecting and Associating Objects from the Organizational Tree

Note: The instructions in this section also refer to querying associated policies by name. In this case, the result of your selection displays the policies associated with the selected objects in the *Policies* window.

This is where you select objects from the Organizational Tree, and from the displayed list select objects for association.

Note:

Before you make your selection in the Tree, you may want to update it. You can either refresh the Tree from SafeGuard PortProtector Management Server, or synchronize it with Active Directory/Novell eDirectory, depending on which Directory you have set SafeGuard PortProtector to use (the Directory may be more up-to-date, but may also take longer). Updating the Tree is done from the Organizational Tree Update menu (shown below) which is found at the top of the Organizational Tree tab.



To update the Organizational Tree from the Management Server:

From the Organizational Tree Update menu, click Refresh Tree. The Tree is updated.

To update the Organizational Tree from the Directory:

From the *Organizational Tree Update* menu, click Sync with Directory. The Tree is updated. This may take a while.

To select the required organizational units:

1 If necessary, expand the Organizational Tree to view lower-level organizational units.

2 Select the required objects by checking the appropriate checkboxes.

3 From the *Object Type* menu below the Organizational Tree

, select the object types you wish to display for the selected objects or **All** if you want to display all types. This means that if, for example, you select a certain Organizational Unit in the Tree, you can then determine with this menu selection which of its members to display (only computers, only users etc.).

Note: When querying associated policies the *Object Type* menu includes only Computers and Users.

4 At the bottom of the *Organizational Tree* tab, click **GO** ( ). The window now displays a table including selected Tree objects and all objects that belong to them.

The Objects table contains a list of the objects that meet your filtering criteria. Each line contains the following columns:

- Checkbox
- Object Name
- Description
- Path

You can modify the table view in the following ways:

- **Sort** the table by clicking the column heading of the column by which you wish to sort. Clicking the header again switch from ascending to descending order. You can add a secondary sort level by pressing the **Shift** key and clicking the secondary column heading.
- **Modify column width** by dragging the column separation lines.
- **Move a column** by dragging and dropping it into the desired position.

To associate a policy with an organizational object:

Note: Instructions 1-3 in this section also refer to querying associated policies by name. In this case, the result of your selection displays the policies associated with the selected objects in the *Policies* window.

1 In the list of objects, select the objects (one or more) to which you wish to associate the policy by checking the appropriate checkboxes.

2 To add the objects to the list of associated objects without closing the window, and to continue adding objects through an additional search, click **Apply**.

3 To add the objects to the list of associated objects and close the window, click **OK**. The objects are added to the list and the *Select Object* window closes. You can now view a list of the associated objects in the bottom part of the *Properties* window.

4 Optional - restrict the policy association to either computers or users within the selected objects as described in *Restricting the Policy to Users/Computers*.

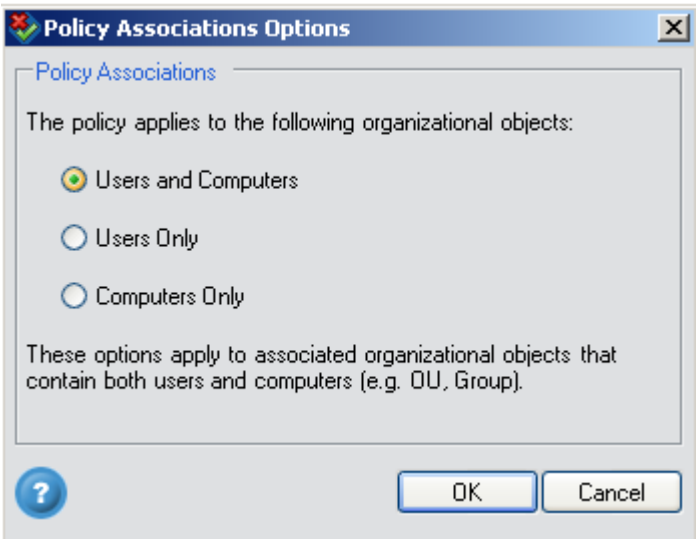
5 Save the policy. The policy will be updated on Clients the next time Clients refresh their policy as determined by the interval you set in the policy's Options settings (see Step *15: Define Options* in *Chapter 3, Defining Policies*).

4.2.4 Restricting the Policy to Users/Computers

Using the Policy Server, it is possible to associate policies to Groups, OUs and Domains, as well as to specific computers and users. When associating a policy to Groups, OUs and Domains that include both users and computers, you can restrict the association only to computers/users within this object. This is typically useful when creating a default machine policy for the entire organization. In such cases, the policy is associated to the entire domain, and is restricted to be applied only to computers.

To restrict a policy to users/computers:

1 Click the **Options** button on the right side of the **Associate Policy with Organizational Objects** bar to display the following window:


Policy Associations Options
Policy Associations
The policy applies to the following organizational objects:
Users and Computers
Users Only
Computers Only
These options apply to associated organizational objects that contain both users and computers (e.g. OU, Group).
OK
Cancel

2 Select the relevant option and click **OK**.

3 The bottom of the **Associate Policy with Organizational Objects** area now indicates this restriction. For example it may read: **This policy applies only to users**. A **Change** link appears to the right of this message enabling you to click it to open the Policy Associations window, shown above.

4.2.5 Disassociating a Policy from Organizational Objects

At times you may wish to disassociate a policy from an organizational object so that it no longer applies to this object.

Note: If the object from which a policy is disassociated needs to be protected, make sure a different policy is applied to it.

To disassociate a policy from an organizational object:

1 In the policy's *Properties* window, in the list of objects that appears in the Associate Policy to Organizational Units section (bottom half of the window), select the object from which you wish to disassociate the policy.

2 Click

OR

1 Right-click the object and select **Delete** from the right-click menu

2 In the *Delete Confirmation* window that opens click **Yes** to confirm delete. The object disappears from the list of associated organizational objects.

3 Save the policy.

Note: Until you save the policy, it continues to apply to the deleted associated object.

4.3 Distributing SafeGuard PortProtector Policies Using Active Directory

SafeGuard PortProtector policies can be distributed, or published, using Microsoft's standard Active Directory GPO distribution feature. To use this feature, first configure the *Administration* window to use Active Directory, as described in Publishing Method in Chapter 7, Administration.

This enables central management of security policies by system administrators and the automatic distribution of policies to existing groups of end-users and computers. There is no need to define user and computer groups and no special configuration or setup is required.

SafeGuard PortProtector automatically creates each policy that you define in SafeGuard PortProtector Management Console as a GPO in Active Directory. These policies are then automatically distributed by Active Directory to the computers and users belonging to the OUs (Organizational Unit) to which you assign them.

The same policy can be distributed to your entire organization, a different policy to each OU or any combination that you require.

Each OU contains a group of computers or users in your organization's domain. For example: the computers in the marketing department or the administrators group. Each computer or user can belong to a single OU. Once you create a policy (GPO) you can link it to an OU. The linked GPO will apply to the computers and users belonging to the OU.

The policy begins protecting the computers following reboot, or after the defined GPO update time interval which is set in your Active Directory has passed. If a protected user logs into a computer, then that user's GPO is applied, meaning that a user policy takes precedence over a computer policy.

Note: You can update policies whenever necessary without waiting for the standard policy distribution time (which is generally 90 minutes). For example, you may want to do this when a specific user needs to use a disk-on-key on a specific computer and cannot wait. This is easily done from SafeGuard PortProtector Management Console, in the Clients World, using the Update Policy option, as explained in *Updating a Policy on a Client* in *Chapter 6, Managing Clients*.

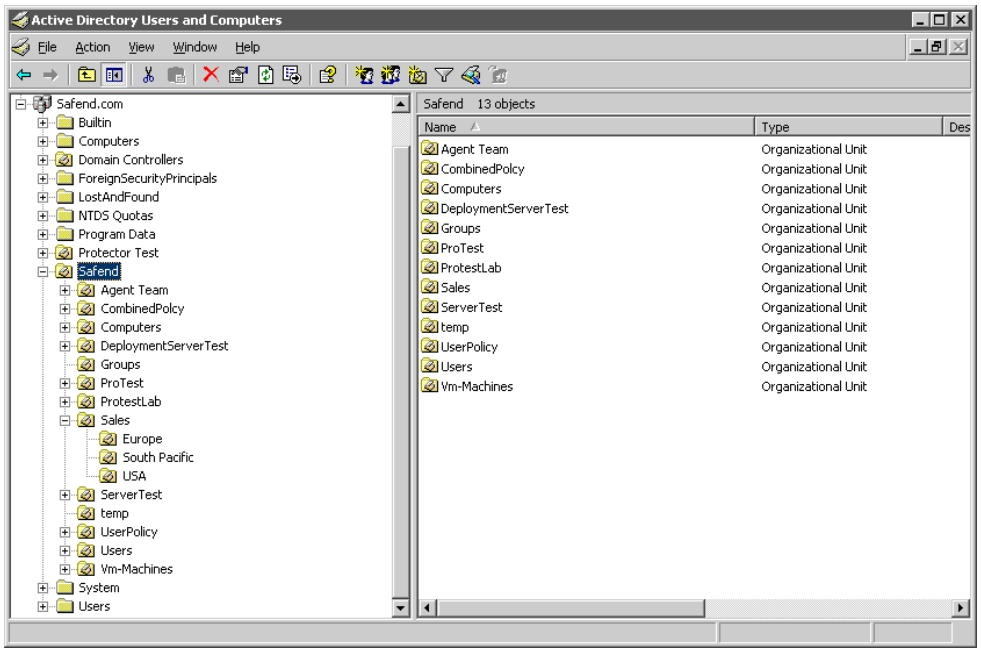
For those of you who are unfamiliar with Active Directory, an explanation of how to link GPOs to OUs follows.

4.3.1 Linking GPO's to Organizational units

This section need be read only by users of Active Directory who are unfamiliar with the process of linking GPOs to OUs in Active Directory.

To link GPOs to OUs:

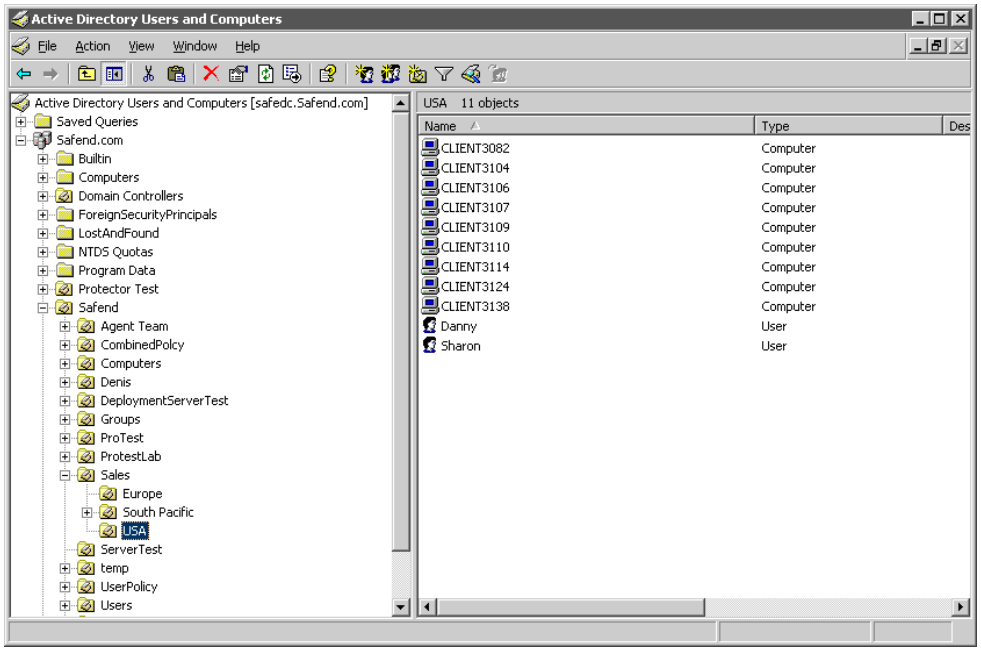
1 Open the Active Directory Users and Computers window by selecting **Start | Programs | Administrative Tools | Active Directory Users and Computers.** An example is shown below:



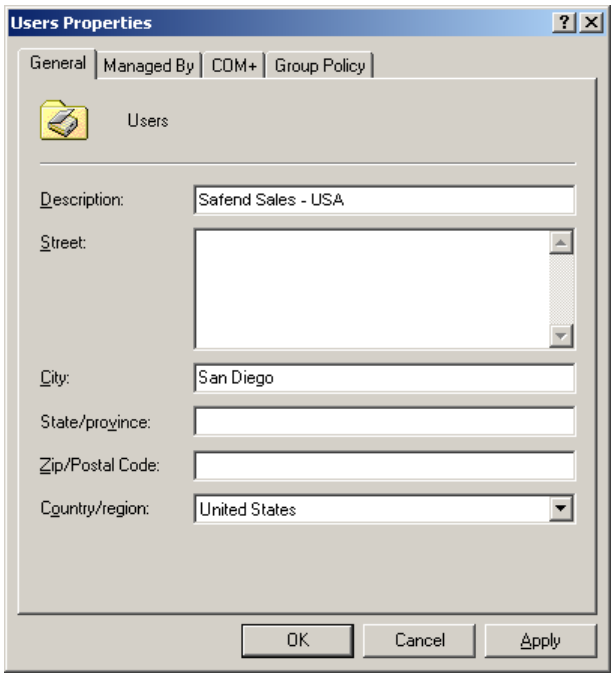
This sample window shows the domain and path where the GPOs are saved in Active Directory. When you install SafeGuard PortProtector, the system automatically detects the domain to which the computer belongs and then creates GPOs under that domain.

The OUs in this Active Directory will appear as folders or sub-folders under that branch. For example: **Sales,** as shown above. These are the OUs to which SafeGuard PortProtector policies will be distributed.

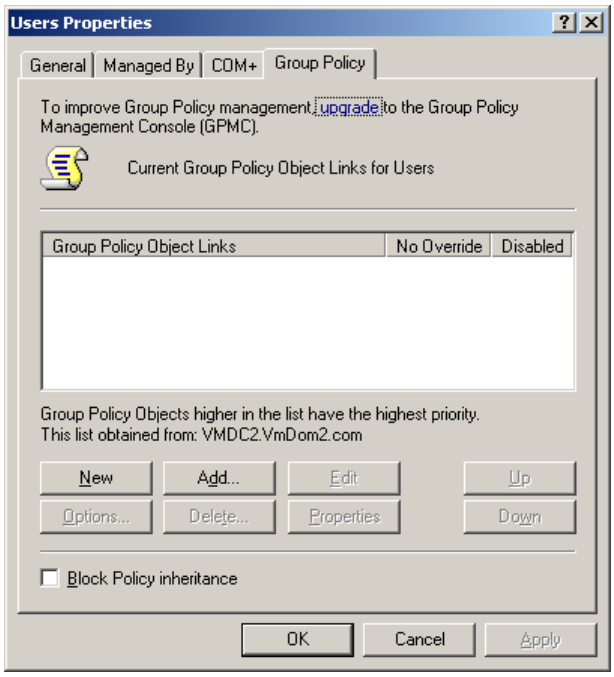
Select a folder to see a list of the actual computers and users that belong to an OU. An example is shown below:



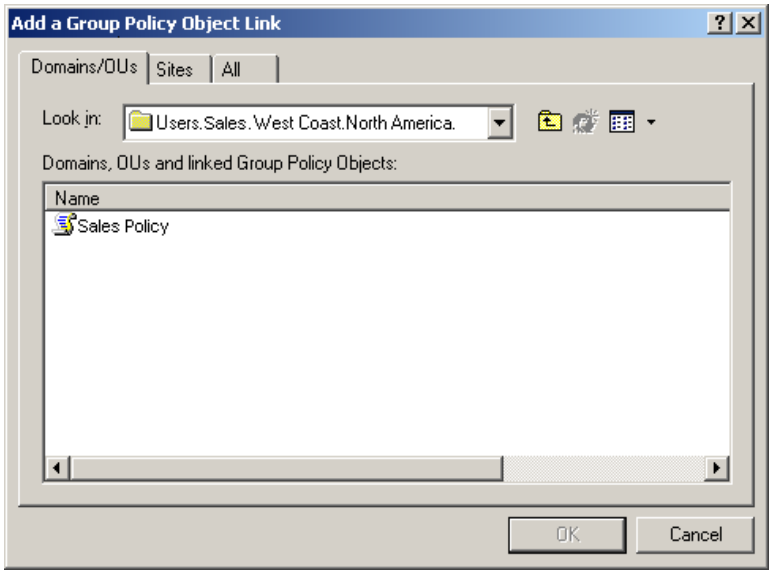
2 Right-click the OU to which you wish to link a GPO and select **Properties**. The following window is displayed:



3 Select the *Group Policy* tab. The following window is displayed:



4 Click the **Add** button. The following window is displayed:



This window lists all the GPOs that are currently linked to this OU.

5 In this window, select the *All* tab. An alphabetical list of GPOs is displayed.

6 From the list, select the policy (GPO) you wish to add to this OU and click **OK**. Once you choose a policy, it is displayed in the *OU Properties* window's *Group Policy* tab and in the OU tree of the *Active Directory Users and Computers* window.
Repeat for each policy which you wish to add to this OU.

7 Click **OK**. These policies are then automatically distributed to the OUs (computers and users) to which you assigned them. You may refer to *Policy Updated* in *Chapter 9, End-user Experience* for a description of the end-user experience when a new policy is distributed.

4.3.1.1 Applying Policies per Security Group

The usual way to apply SafeGuard PortProtector Policies (GPO's) is to objects that reside in an OU container (computer or user). In some large scale organizations this might be cumbersome, and difficult to manage. Another option is to apply the policy to users that reside in security groups, in a process called security filtering.

A good example of an organization which could use this method is an organization which contains all users in one OU, and all computers in another OU (in the domain).

In this case it would be easier to use existing security groups and apply the policy to them than to rearrange the computers/users in a new OU structure.

Security filtering is essentially a procedure by which you apply several GPO's to the same OU (which contains users) and then change the ACE (access control entries) on those GPO's to only allow users in certain security group to read and apply that specific Protector/Group Policy.

Default ACE entries for a new Group Policy Object:

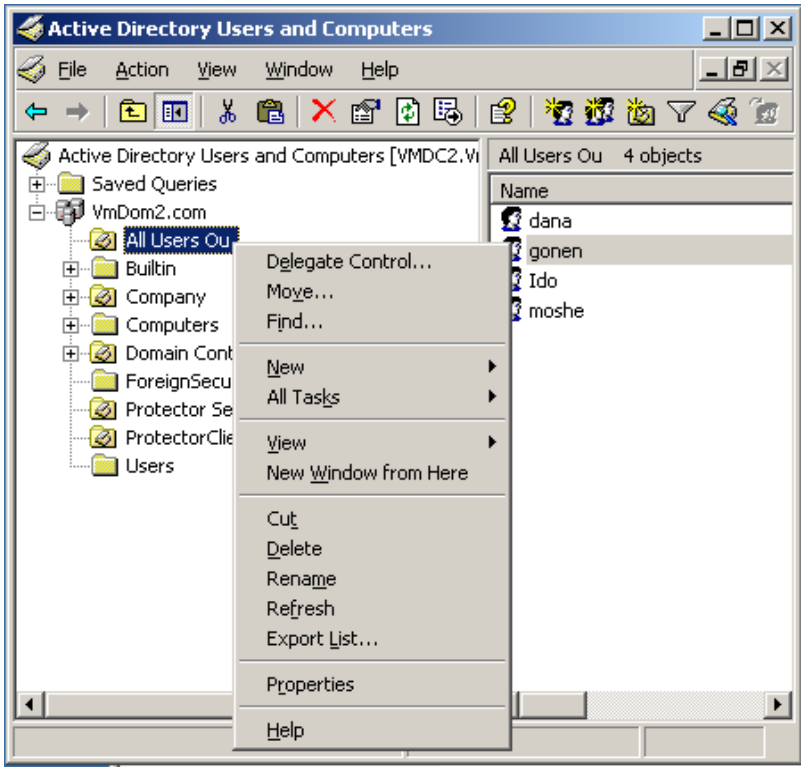
Security Principal	**Read**	**Apply Group Policy**
Authenticated users	Allow	Allow
Creator owner	Allow (implicit)	
Domain admins	Allow	
Enterprise admins	Allow	
Enterprise domain controllers	Allow	
System	Allow	

In order to apply security filtering, we need to create the desired SafeGuard PortProtector policies and save them as GPO's in Active Directory, as we would in any case. These new policies need to be linked to the OU which contains all the users.

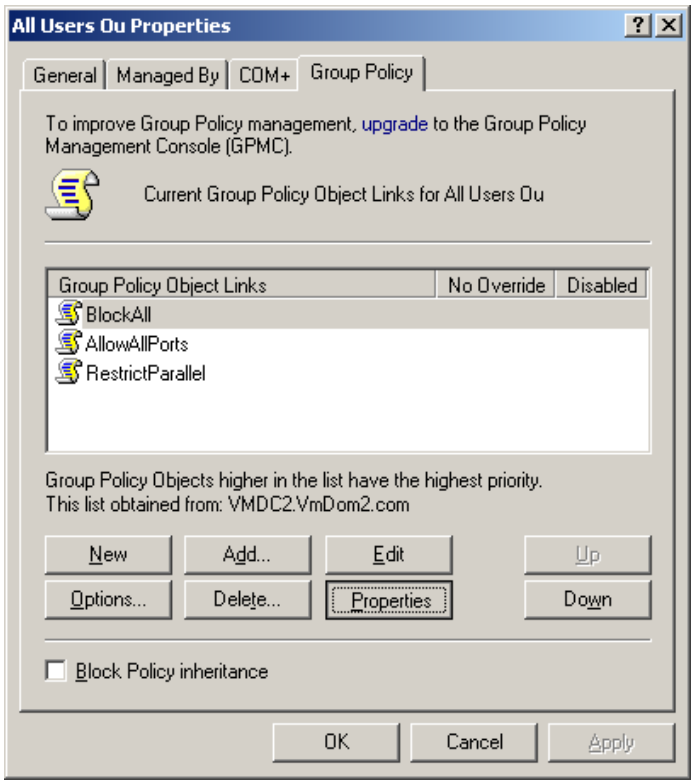
For example, we might want to apply a block all ports policy we created (named BlockAll) to users who reside in a security group called BlockAll.

To change the ACE in the BlockAll Policy:

1 Open the *Active Directory Users and Computers* window, right-click the OU containing all the users and select "Properties".

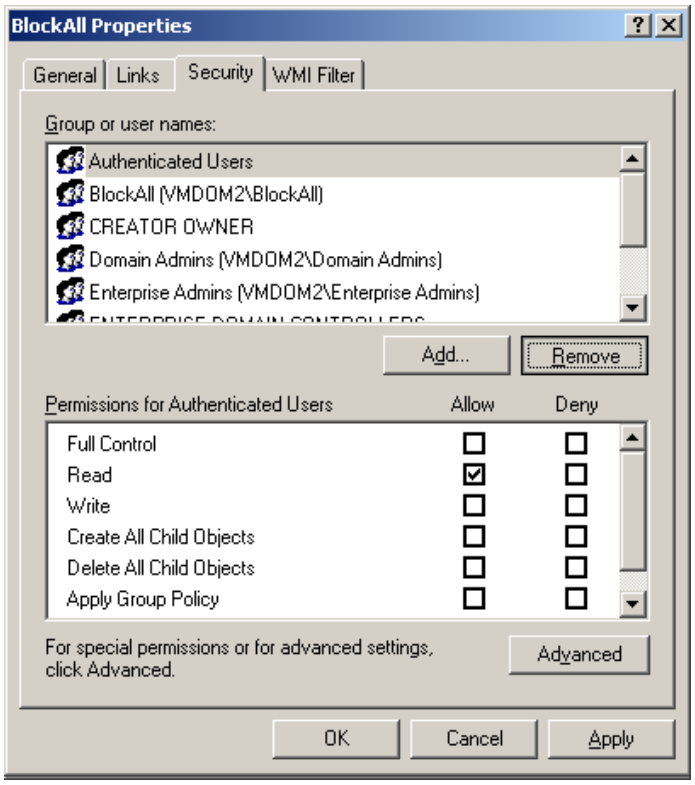


2 Navigate to the *Group Policy* tab:



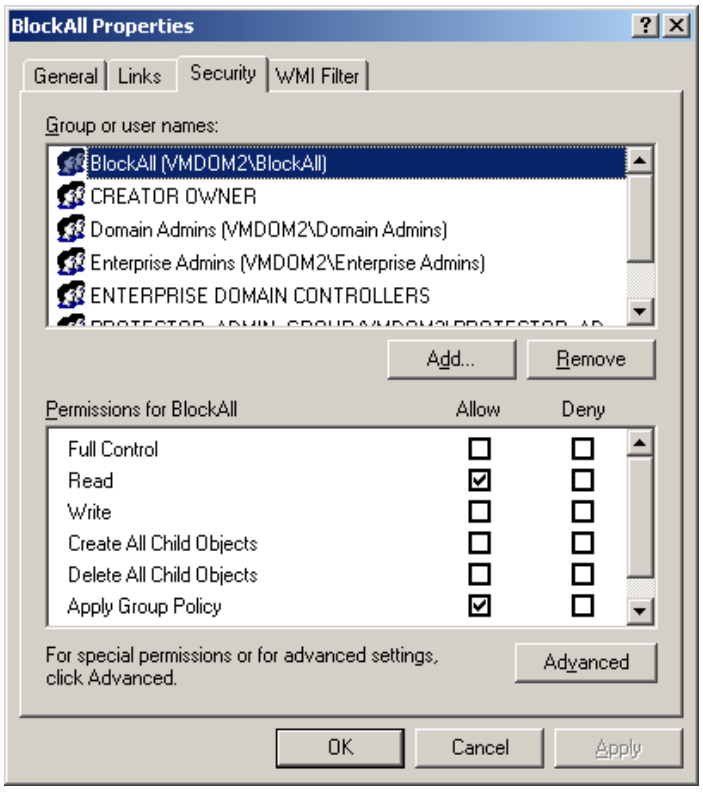
3 Select the BlockAll Policy and click **Properties.**

4 Navigate to the *Security* tab:



5 Remove Authenticated Users from the ACE.

6 Add the BlockAll security group and give it **Read** and **Apply Group Policy** permissions as shown below:



7 Click **OK** to save the new settings.

4.4 Distributing SafeGuard PortProtector Policies Using Registry Files

Using registry files allows you to use other management applications for distributing policies, in cases where you do not wish to use the Policy Server or the Active Directory GPO mechanism, or do not have the infrastructure to do so.

This option stores registry files in a shared folder and enables you to use third-party tools to publish SafeGuard PortProtector policies to the SafeGuard PortProtector Clients. When this option is used, SafeGuard PortProtector generates two copies of the registry file, one suitable for computers (for example: **MyPolicy(MACHINE).reg**) and one suitable for users (for example: named **MyPolicy(USER).reg**).

To distribute a policy to a Client using .reg files:

1 Double-click the required .reg file and click **Yes** in the confirmation window to add its information to the registry.

2 Update the policy on the Client as explained in Updating the Client's Policy in 8, End-user Experience.

Often, you may want to automate the process in which policies are distributed by a third party tool (i.e. SMS, Novell eDirectory) after editing/creating policies. Refer to *Run Executable after Publish* in *Chapter 7, Administration* for more details.

4.5 Policy Merging

When more than one policy is associated with an organizational object, the definitions in all the associated policies may be merged so as to produce the definition that will be enforced on the endpoint. A typical example of using this capability is defining a general policy for a specific department, and another policy for a specific user in that department who requires additional permissions. Depending on the selected policy distribution method, policy merging happens as follows:

Using the Policy Server - policy merging is automatic.

Using Active Directory – policy merging is optional and is defined in Configuring Policies Tab Settings in *Chapter 7, Administration*.

Using registry files – policy merging is not possible.

Policy merging works as follows:

- **Permissions**: for each port/device/storage device/file type/WiFi link, the most permissive definition of all merged policies is applied (for an explanation of the order of permissiveness refer to *Storage Control - White List Tab* in *Chapter 3, Defining Policies*). However, there are few exceptions to the **Most permissive apply rule** that are specified below.
- **Settings**: For each type of setting (Logging, Alerts etc.) the definitions are taken from the policy whose name is first alphabetically.

  Note:

  When merging policies it is recommended that you use Global Policy Settings rather than policy-specific settings in order to avoid misconfiguration of policy settings, which are taken only from one policy.

Example 1:

Merged policies are PolicyA and PolicyB:

PolicyA permission for removable storage devices is **Allow**.

PolicyB permission for removable storage devices is **Encrypt**.

PolicyA and PolicyB have different Settings.

If we merge PolicyA and PolicyB on an endpoint, the **Allow** permission will apply for removable storage devices, since **Allow** is more permissive than **Encrypt**.

Since PolicyA and PolicyB have different Settings, the Settings are taken from the definitions in PolicyA as it is the first alphabetically.

Example 2:

Merged policies are PolicyA and PolicyB:

PolicyA permission for removable storage devices is **Allow**.

PolicyB permission for removable storage devices is **Read Only**.

If we merge PolicyA and PolicyB on an endpoint, the **Allow** permission will apply for removable storage devices, since **Allow** is more permissive than **Read Only**.

Example 3:

Merged policies are PolicyA and PolicyB:

PolicyA permission for disk on key Smart Functionality is **Allow**.

PolicyB permission for removable storage devices is **Block**.

If we merge PolicyA and PolicyB on an endpoint, the **Allow** permission will apply for disk on key Smart Functionality, since **Allow** is more permissive than **Block**.

Example 4:

Merged policies are PolicyA and PolicyB:

PolicyA permission for disk on key Smart Functionality is **Allow**.

PolicyB permission for removable storage devices is **Block**.

If we merge PolicyA and PolicyB on an endpoint, the **Allow** permission will apply for disk on key Smart Functionality, since **Allow** is more permissive than **Block**.

Note: When policies are merged on a Client, the names of all merged policies are displayed in this Client's logs and its information in the Clients Table.

4.5.1 Policy Merging When Unclassified Devices are Allowed

When unclassified devices are defined as **Allowed** in the *Policies* page of the *Administration* window, as described in

Allowing / Blocking Access to Unclassified Devices, policy merging behaves differently with respect to Device Control.

In this case, the most restrictive Device Control definitions of all merged policies are enforced. This means that the security actions defined in the **Device Control** tab of the policy are merged so that the most restrictive take effect, while the rest of the policy definitions (such as: Port Control, Storage Control and File Type Control) are still merged so that the most permissive security actions take effect, as described above.

This enables the administrator to gradually restrict the devices in different parts of the organization as SafeGuard PortProtector is assimilated in the organization.

Note: When unclassified devices are defined as **Allowed** in the *Policies* page of the *Administration* window, it will affect the *Device Control* window in the *General* tab of the *Policy* window. The *Device Control* window will show **Allow** (✔) in the **Devices Not Approved in Device Types or White List** area for *Unclassified Devices* at the bottom of the window. This indicates that unclassified devices are allowed and that Device Control policy merging has been affected, as described above.

Example:

The following example demonstrates how Device Control and Storage Control behave when unclassified devices are defined as **Allowed** in the *Policies* page of the *Administration* window.

The merged policies are Policy A and Policy B, as follows:

In Policy A, Device Control specifies that printing devices are allowed.

In Policy A, Storage Control specifies that removable storage devices are allowed.

In Policy B, Device Control specifies that printing devices are blocked.

In Policy B, Storage Control specifies that removable storage devices are blocked.

If we merge Policy A and Policy B for a specific endpoint, then printing devices will be blocked because the most restrictive Device Control security actions takes effect, and block is more restrictive than allow.

Removable storage devices will be allowed because the most permissive Storage Control security actions takes effect, and allow is more permissive than block (since the security actions of removable storage devices are a Storage Control definition and not a Device Control definition, they are still merged in the standard, most permissive manner).

4.5.2 Policy Merging when Other File Types are Allowed

When **Other File Types** are defined as **Allowed** in the **File Type Control** tab of the policy, policy merging behaves differently with regard to file control.

In this case, the most restrictive File Type Control definitions of all merged policies are enforced. This means that the security actions defined in the **File Type Control** tab of the policy are merged so that the most restrictive take effect, while the remainder of the policy definitions (such as: Port Control, Device Control, Storage Control and WiFi Control) are still merged so that the most permissive security actions take effect, as described above.

Example:

Policy A and Policy B are two merged policies.

Policy A specifies that the permission for writing Other File Types is **Blocked** and that for writing File Type Published Documents is **Blocked**.

Policy B specifies that the permission for writing Other File Types is **Blocked** and that for writing File Type Published Documents is **Allowed**.

If Policy A and Policy B are merged on an endpoint, then the **Allowed** permission for Published Document will apply, since Other File Types are set to **Blocked** so that the most permissive definition for file groups applies, including Published Documents.

5 Viewing Logs

About This Chapter

This chapter describes The Logs World, which enables you to view, manage and collect SafeGuard PortProtector logs and shadowed files, as well as perform some administrative tasks. The chapter contains the following sections:

- ***Overview*** describes logs and their function and provides a quick tour of the Logs World.
- ***Quick Tour of the Logs World*** describes the main window of the Logs World.
- ***The Log Table*** describes the Log Table and its contents, and how you can manage and navigate it.
- ***Filtering by Log Record Origin*** describes the way you can filter the Log Table to display logs only for selected organizational units, computers or users.
- ***Queries*** describes the queries that provide an additional method for filtering the Log Table.
- ***Active Window Options*** discusses duplicating, undocking and closing a window.
- ***Collecting Logs*** describes how to collect logs at any time without having to wait for the log collection interval to complete.
- ***Tracking Client Task Progress*** describes how to track the progress of Client tasks such as log collection and policy update.
- ***Log Table Structures*** describes the structure of Client, File and Server log tables.

5.1 Overview

Events that occur on endpoints protected by SafeGuard PortProtector Clients are recorded in logs and/or alerts. An event may be a connection or a disconnection of a device, connection to a wireless network, tampering attempts or administrator login, to name but a few. These events are stored as Client logs. Logs/alerts recording the name of a file read from or written to storage devices are stored as File logs.

Client and File Logging logs and alerts may refer to a computer or to a user, depending on how the policy that dictates them is applied.

In addition to events which occur on protected endpoints, logs and alerts are also created by SafeGuard PortProtector Management Server events such as administrator login, publishing policies and performing backups.

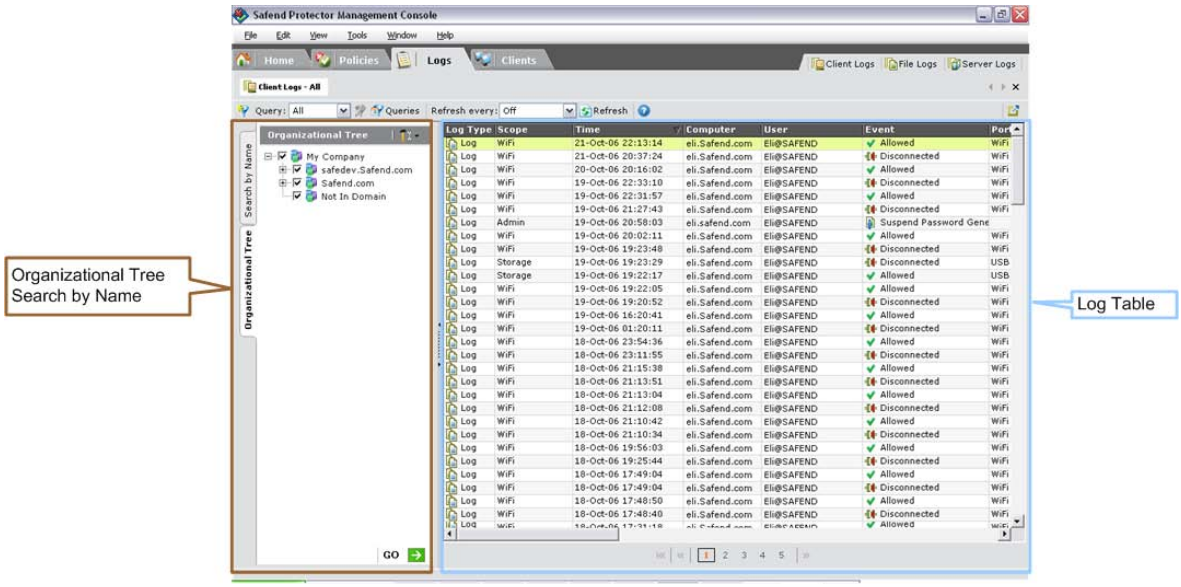
Client and Server logs and alerts are sent to a log repository on the Management Server at intervals as defined in the Client's policy, and stored there. If necessary, they can also be collected by the administrator at other times. This chapter describes the Logs World, which provides various options for querying and viewing logs and alerts.

5.2 Quick Tour of the Logs World

This tour refers to Client logs and File logs. Server log windows differ in that they do not have an Organizational Tree section.

To access the Logs World:

Click the **Logs** tab. The Logs window appears:



The Logs World window includes the sections and control buttons described in *Know* Your Way around the Application in *Chapter 2, Getting Started*. The launch buttons and some of the menu options are particular to the Logs world.

5.2.1 Launch Buttons

The launch buttons particular to the Logs World include the following:

- **Client Logs**

– clicking this button opens a new Client Logs window displaying logs for the current Organizational Tree selection (refer to *Filtering by Log Record Origin* for an explanation of the Organizational Tree).
- **File Logs**

– clicking this button opens a new File Logs window displaying logs for the current Organizational Tree selection (refer to *Filtering by Log Record Origin* for an explanation of the Organizational Tree).
- **Server Logs**

– clicking this button opens a new Server Logs window displaying Server logs.

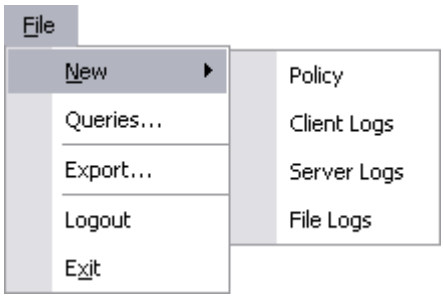
Client, File and Server logs are explained in *The Log Table*.

5.2.2 Menus

Some of the menu options in the Logs World are particular to this world. A description of each menu and its options follows.

5.2.2.1 File Menu

The *File* menu in the Logs World enables you to open other World windows, manage queries, export queries and more.



The *File* menu in the Logs World includes the following options:

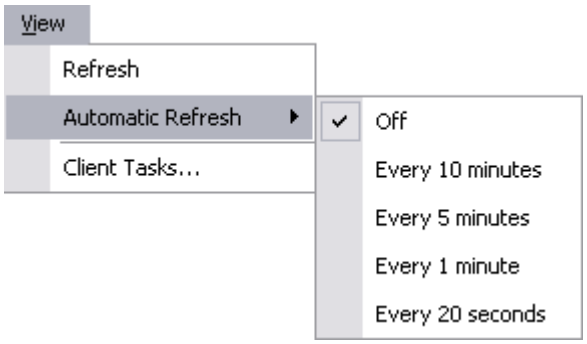
Option	Description
New	Opens a submenu that enables you to open a new policy window, a new Clients Log window, a new Server Log window or a new File Log window or a new report.
Queries	Enables you to manage queries.
Export	Exports the query to an external file.
Change User Role	A SafeGuard PortProtector administrator can be assigned more than one role in order to define the various domain partitions for which they are responsible. After such an administrator logs in, a selection window is automatically displayed for selecting the role in which to work. **Note:** A User Role defines the functions, OUs and domains of an organization to which a SafeGuard PortProtector administrator has access, as described in *Defining Roles*. The **Change User Role** option enables such an administrator to change this role at any time to another role that has been assigned to him or her.
Logout	Logs the current user out of the Management Console.
Exit	Logs out the current user and closes SafeGuard PortProtector Management Console

5.2.2.2 Edit Menu

The *Edit* menu in the Logs World is disabled.

5.2.2.3 View Menu

The *View* menu enables you to refresh the *Logs* window which displays a list of your logs and to view the progress of Client tasks.



The *View* menu includes the following options:

Option	Description
Refresh	Updates the log to provide you with an up to date view.
Automatic Refresh	Opens a sub-menu that allows you to determine how often the active log type (*Client*, *file* or *server*) should be automatically refreshed.
Client Tasks	Displays the progress of Client tasks.

5.2.2.4 Tools Menu

The *Tools* menu which is common to all Worlds is described in *Tools Menu* in *Chapter 2, Getting Started*.

5.2.2.5 Window Menu

The *Window* menu which is common to all Worlds is described in *Window* Menu in Chapter 2, Getting Started.

5.2.2.6 Help Menu

The *Help* menu which is common to all Worlds is described in help menu in Chapter 2, Getting Started.

5.2.3 Toolbar

The toolbar provides quick access to some commonly used functions. It appears below the Windows bar, and includes the following buttons:

The following is a brief description of each toolbar button:

Button	Description
New Query	Opens a new *Query Properties* window (for more about queries see *Queries*).
Query Menu	Allows query selection from drop down menu (for more about queries see *Queries*).

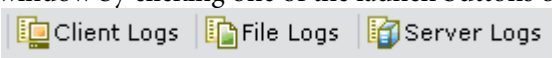
Button	Description
Edit Query	Opens properties of the applied query for editing.
Manage Query	Opens the *Manage Queries* window (for more about queries see *Queries*).
Refresh	Refreshes the Log Table in the active window.
Automatic Refresh	Sets the Log Table to refresh at the given interval.
Help	Displays the context sensitive help of the active window, and enables access to other help topics.

5.2.4 Workspace

The workspace is divided into two areas:

- The **Log Table** appears in the right-hand pane and displays a table of log records received from Clients or from the Management Server. When opened initially the table displays all Client logs. The Log table is discussed in *The Log Table.*
- The area on the left-hand pane includes the **Organizational Tree** and **Search By Name** tabs on the left pane. These tabs serve as filters for determining the origin (i.e. organizational units/computers/users) of log records displayed in the Log Table. The tabs are discussed in *Filtering by Log Record Origin*.
  These tabs does not appear in the Server log window, since by definition Server logs do not apply to Clients.

When all windows in the Logs World are closed, the workspace is empty. You may open a log window by clicking one of the launch buttons on the top right-hand side of the window:

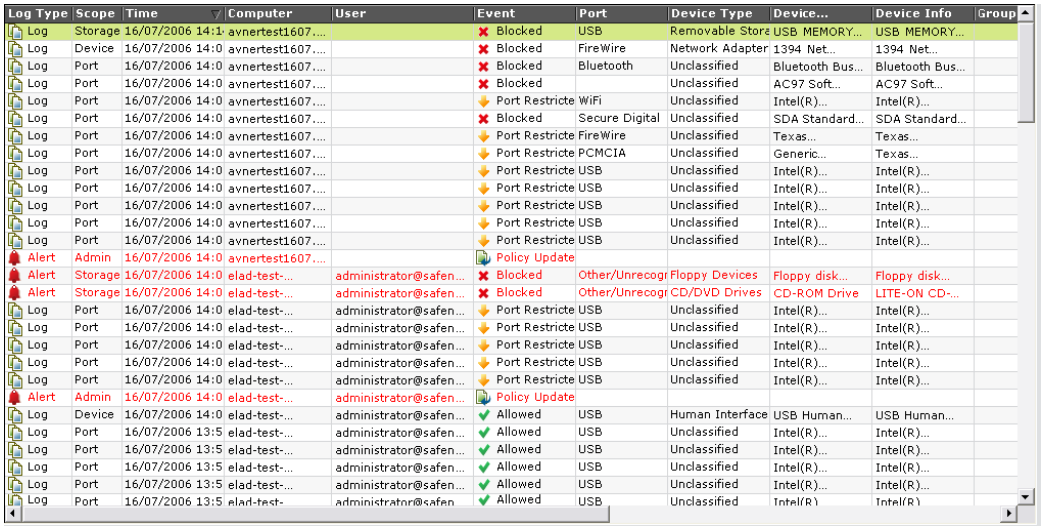


Refer to *The Log Table* to learn about viewing logs.

5.3 The Log Table

The log table (shown in the figure below) displays information about events that take place in SafeGuard PortProtector Clients, Management Consoles or Management Server. There are three types of Log Tables which you can view and manage:

- **Client Log** – this log displays information about Clients and users in the organization. Each record reports a specific event, such as the connection of a detachable device to a computer, a tampering attempt and so on. Refer to *Client Log Structure* for a description of the log structure.
- **File Log** – if the file logging feature is activated for removable storage devices, external hard disks or CD/DVD, then the file information is displayed in this log. Refer to *File Log Structure* for a description of the log structure. File Shadowing logs are also shown here.
- **Server Log** – this log displays information about the Management Server and administrative actions. Each record reports a specific event, such as logging into the Management Console, changing Global Policy Settings and more. Refer to *Server Log Structure* for a description of the log structure.



Log Type	Scope	Time	Computer	User	Event	Port	Device Type	Device...	Device Info	Group
Log	Storage	16/07/2006 14:1	avnertest1607....		Blocked	USB	Removable Store	USB MEMORY...	USB MEMORY...	
Log	Device	16/07/2006 14:0	avnertest1607....		Blocked	FireWire	Network Adapter	1394 Net...	1394 Net...	
Log	Port	16/07/2006 14:0	avnertest1607....		Blocked	Bluetooth	Unclassified	Bluetooth Bus...	Bluetooth Bus...	
Log	Port	16/07/2006 14:0	avnertest1607....		Blocked		Unclassified	AC97 Soft...	AC97 Soft...	
Log	Port	16/07/2006 14:0	avnertest1607....		Port Restricte	WiFi	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 14:0	avnertest1607....		Blocked	Secure Digital	Unclassified	SDA Standard...	SDA Standard...	
Log	Port	16/07/2006 14:0	avnertest1607....		Port Restricte	FireWire	Unclassified	Texas...	Texas...	
Log	Port	16/07/2006 14:0	avnertest1607....		Port Restricte	PCMCIA	Unclassified	Generic...	Texas...	
Log	Port	16/07/2006 14:0	avnertest1607....		Port Restricte	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 14:0	avnertest1607....		Port Restricte	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 14:0	avnertest1607....		Port Restricte	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 14:0	avnertest1607....		Port Restricte	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 14:0	avnertest1607....		Port Restricte	USB	Unclassified	Intel(R)...	Intel(R)...	
Alert	Admin	16/07/2006 14:0	avnertest1607....		Policy Update					
Alert	Storage	16/07/2006 14:0	elad-test-...	administrator@safen...	Blocked	Other/Unrecogr	Floppy Devices	Floppy disk...	Floppy disk...	
Alert	Storage	16/07/2006 14:0	elad-test-...	administrator@safen...	Blocked	Other/Unrecogr	CD/DVD Drives	CD-ROM Drive	LITE-ON CD-...	
Log	Port	16/07/2006 14:0	elad-test-...	administrator@safen...	Port Restricte	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 14:0	elad-test-...	administrator@safen...	Port Restricte	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 14:0	elad-test-...	administrator@safen...	Port Restricte	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 14:0	elad-test-...	administrator@safen...	Port Restricte	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 14:0	elad-test-...	administrator@safen...	Port Restricte	USB	Unclassified	Intel(R)...	Intel(R)...	
Alert	Admin	16/07/2006 14:0	elad-test-...	administrator@safen...	Policy Update					
Log	Device	16/07/2006 14:0	elad-test-...	administrator@safen...	Allowed	USB	Human Interface	USB Human...	USB Human...	
Log	Port	16/07/2006 13:5	elad-test-...	administrator@safen...	Allowed	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 13:5	elad-test-...	administrator@safen...	Allowed	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 13:5	elad-test-...	administrator@safen...	Allowed	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 13:5	elad-test-...	administrator@safen...	Allowed	USB	Unclassified	Intel(R)...	Intel(R)...	
Log	Port	16/07/2006 13:5	elad-test-	administrator@safen	Allowed	USB	Unclassified	Intel(R)	Intel(R)	

The figure above shows the Clients log. File logs and Server logs display different information.

By default, the initial Log Table displays the Clients Log, containing all record types for all the Clients and users in the organization. You can open additional windows with additional log types – Client Logs, Server Logs or File Logs. A detailed explanation of the table structures can be found at the end of this chapter in *Log Table Structures*.

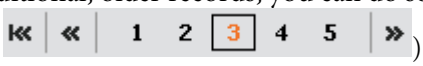
You can modify the table view in the following ways:

- **Sort** the table by clicking the column heading of the column by which you wish to sort. Clicking the header again switch from ascending to descending order. You can and a secondary sort level by pressing the **Shift** key and clicking the secondary column heading.
- **Modify column width** by dragging the column separation lines.
- **Move a column** by dragging and dropping it into the desired position.

Whichever log type you choose to view, the number of records displayed may be overwhelming, and some of these records may not be relevant. There are, therefore, two ways in which this number can be decreased:

- **Filtering by Log Origin**: this allows you to limit log records to those originating from specific computers/users or organizational units. For an in-depth discussion of these options see *Filtering by Log Record Origin*, which discusses the Organizational Tree and the Search by Name tabs (these are not applicable to Server Logs).
- **Queries**: queries can be created in order to select records according to various parameters such as record type, time, device type and more. For an in-depth discussion of queries see *Queries*.

5.3.1 Viewing Additional Records

The Log Table displays the first 1000 records that answer your query/filtering criteria. If you wish to view additional, older records, you can do so using the paging buttons that appear below the Log Table. (

).

To navigate to older or newer log records:

Use the paging buttons that appear below the Log Table. You may either click a specific page number, or click **Next Page** (»), **Previous Page** («) or **First Page** (⏮) to navigate between log pages.

Note: Displaying a new page may take a while as it may require loading new data from the database.

Note: Automatic Refresh is disabled while you view pages 2 and up of the Log Table.

5.3.2 Refreshing the Log Table

The Log Table refreshes automatically at predefined intervals which you determine, or as a response to an ad hoc request. The refresh process collects new data accumulated on the Management Server and then displays them in the Log Table in accordance with the current table sorting definition.

To refresh the Log Table:

In the *View* menu, click **Refresh**, or click the **Refresh** icon ( ) in the toolbar. New log records are added to the log table.

To set automatic refresh intervals:

Select the interval from the **Refresh every** drop-down menu in the Toolbar.

OR

1 In the *View* menu, point to **Automatic Refresh**. A sub menu opens.

2 In the sub-menu, click the desired refresh interval.

3 From this moment onward the table refreshes at the selected interval.

Note: Automatic Refresh of the Log Table is disabled while you view pages 2 and up of the table.

5.3.3 Log Record Options

In the Log Table, several options are available with regards to log records. These options enable you to do the following:

- View record properties.
- Open the policy with which a log record is associated.
- Copy USB device information to the clipboard.
- Show all logs for device/policy/user/computer with which a log record is associated.

These options are explained in the following sections.

To access log record options:

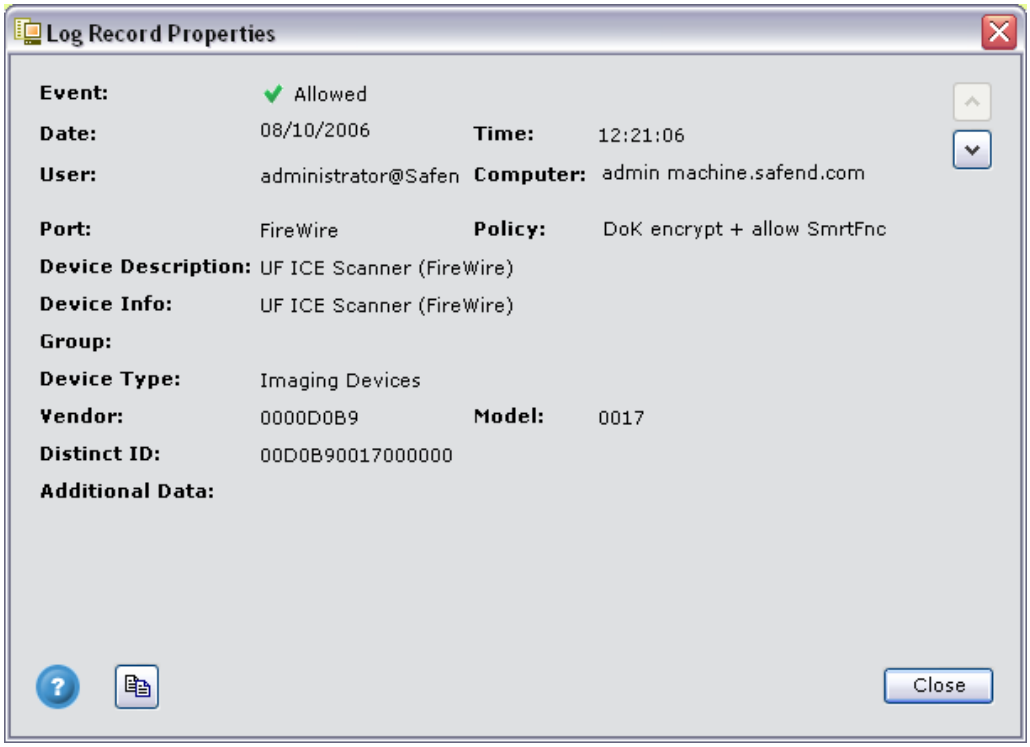
In the Log **Table**, right-click the required record. A menu opens.

5.3.3.1 Viewing Log Record Properties

This option allows you to view record properties in a window instead of scrolling across the Log Table.

To view record properties:

In the right-click menu, click **Properties**. The *Log Record Properties* window opens:



5.3.3.1.1 Log Record Properties

This window displays the record's fields, depending on the record type, and their value. For each log type (Client, File or Server) different information is displayed, as in the relevant table columns. For an explanation of the fields please see the following:

- **Client Log Properties** - refer to *Client Log Structure*.
- **File Log Properties** – refer to *File Log Structure*.
- **Server Log Properties** – refer to Server Log Structure

You can move to the previous or next record from within the *Log Record Properties* window by using the up and down arrows at the top right-hand side of the window.

If the log record refers to a USB device or to a CD/DVD medium, the **Copy** button at the bottom left of the window is enabled. This allows you to copy the device or medium information to the clipboard and then paste it into a group in the White List.

To copy USB device or CD/DVD medium information to the clipboard:

Click the **Copy** button at the bottom left of the window. The device/medium details are copied to the clipboard and can be pasted in the Policies World, into a group in the White List.

To View a Shadowed File:

Select **Open** or **Save** in the Shadow File column to download the shadowed file from the repository.

5.3.3.2 Opening Applied Policy

This option allows you to open the policy that caused the SafeGuard PortProtector Client to send the log, in order to view its definitions.

To open the policy:

In the right-click menu, click **Open Policy**. The application switches to the *Policies* world, displaying the policy applied on the Client that sent the log record.

Note: In the case of merged policies (see *Policy Merging*) the policy whose name is first alphabetically is opened.

5.3.3.3 Copying Record USB Device or CD/DVD Medium Information

This option allows you to copy the information regarding the USB device or CD/DVD medium associated with this log record to the clipboard in order to paste it later when approving this device/medium in a policy (refer to *Approving Devices and WiFi Connections or Approving CD/DVD Media* in *Chapter 3, Defining Policies*).

To copy device/medium information:

In the right-click menu, click **Copy USB Device Information**. The device/medium details are copied to the clipboard and can be pasted in the Policies World, into a group in the White List (see *Adding Devices* and *Adding Media* in *Chapter 3, Defining Policies*).
This can also be done from the *Log Record Properties* window.

5.3.3.4 Showing All Associated Log Records

Through this option you can view all log records associated with the same device, policy, user, or computer with which the selected record is associated.

To view all associated logs:

1 In the right-click menu, click **Show All Logs.** A sub-menu opens.

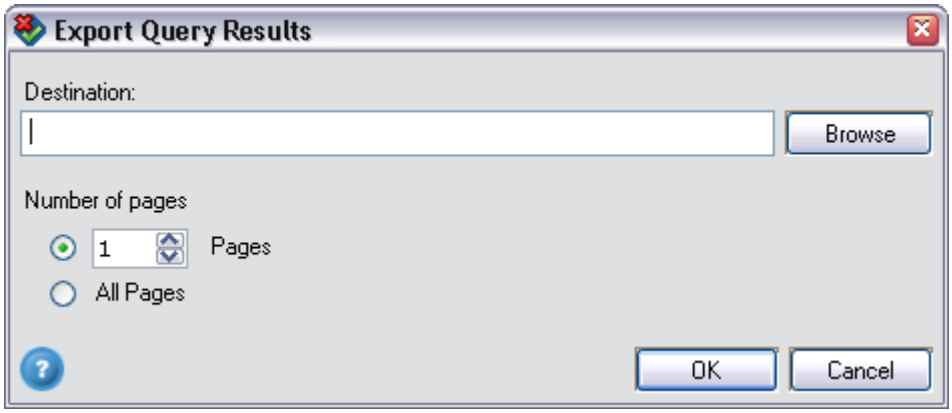
2 From the sub-menu, select the log records (From this device, From this policy, Of this user, Of this computer) you wish to view. The Log Table now displays all records for the selected type.

5.3.4 Exporting the Log Table

The Log Table can be exported using the *Export Query Results* window.

To open the *Export Query Results* window:

From the *File* menu, select **Export**. The *Export Query Results* window opens:



5.3.4.1 Exporting Query Results

Use this option to export the Log Table (i.e. the query results) in order to print it or perform further analysis you can do so. The file is saved in XML format which can easily be opened with MS Excel etc.

To export query results:

1 Click **Browse** button to select a path or type in the path for the exported file. You may use the default file name or change it.

2 If you want to select only the latest records of the query results, click the first radio button and select how many pages you wish to export.

3 If you want to export all query result pages, select the **All Pages** radio button.

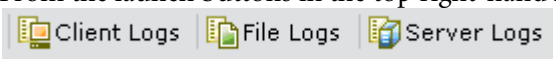
Note: Exporting the entire query may take a long time.

4 Click **OK**. A progress window opens, and exporting begins.

5.3.5 Viewing Additional Log Tables

For your convenience, you may open additional Log windows and view several Log windows concurrently. There are several ways in which you can do this:

To open a new log window:

From the launch buttons in the top right-hand launch tab of the Log World tab (

) click the desired launch button

OR

From the *Manage Queries* window (see *Managing Queries*).

OR

From the File menu, select **New**. A secondary menu opens.

From the secondary menu, select the type of window you wish to open (Client Logs, Server Logs or File logs).

The requested log window opens.

5.4 Filtering by Log Record Origin

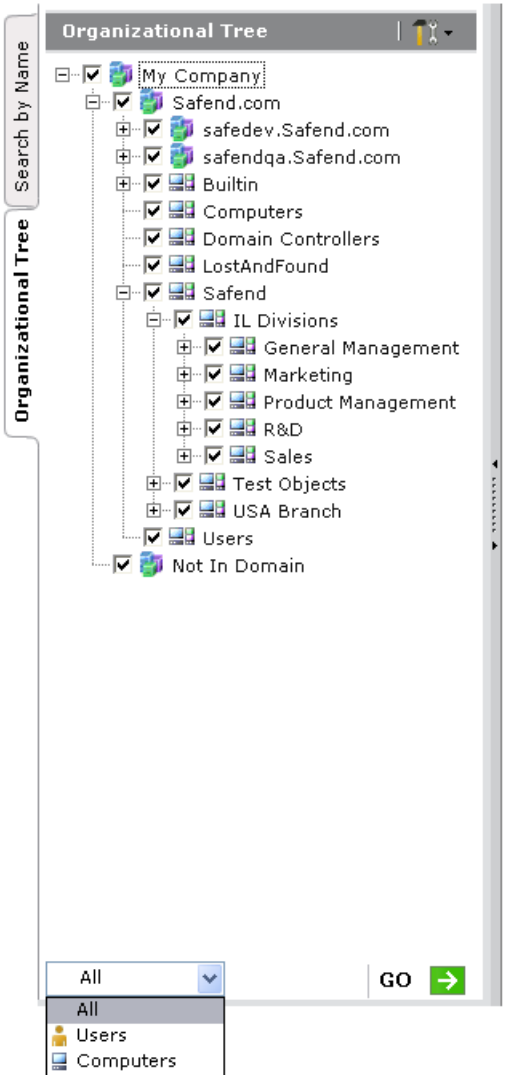
The left-hand side of the main Logs window includes two tabs to help you determine the organizational units or computers/users whose logs will be displayed in the Log Table. These are the Organizational Tree tab and the Search by Name tab. This section does not apply in the case of Server logs.

5.4.1 Filtering the Log Table by Organizational Unit

The *Organizational Tree* is a tool you use to determine the Organizational Units whose log records will be displayed in Client or File logs. Together with queries (see *Queries*), selection of items in the Organizational Tree determines which records are displayed in the Log Table (see *The Log Table*). This section describes how to manage the Organizational Tree and how to determine, from the Tree, which logs and alerts to display in the Client or file Log Table.

As mentioned, the Tree does not appear in the Server log window, since by definition Server logs do not apply to computers or users.

The *Organizational Tree* tab displays the domain(s), organizational units and the Not In Domain group (which includes all computers who do not currently belong to any domain), as shown in the following figure:



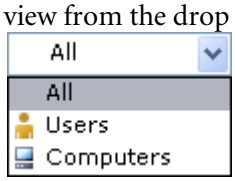
Note: The Organizational Tree is applicable only if you are using Active Directory or Novell eDirectory. If you are not, only one group is displayed in the Tree – Not In Domain. Selecting this group selects all computers.

To select the required organizational units:

1 If necessary, expand the Organizational Tree to view lower-level organizational units.

2 Select the required domain or organizational units by checking the appropriate checkboxes.

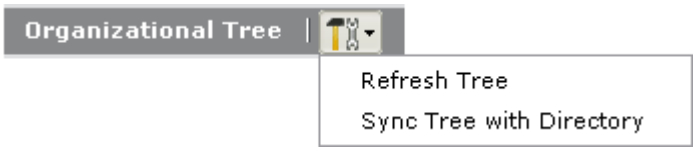
3 At the bottom of the *Organizational Tree* tab, select the type of objects you would like to view from the drop down menu



4 At the bottom of the *Organizational Tree* tab, click **GO** ( ). The logs now displayed in the log table originate from Clients that belong to your Tree selection, and only them.

5.4.1.1 Updating the Organizational Tree

Before you make your selection in the Tree, you may want to update it. You can either refresh the Tree from SafeGuard PortProtector Management Server, or synchronize it with Active Directory/Novell eDirectory (the Directory may be more up-to-date, but may also take longer). Updating the Tree is done from the *Organizational Tree Update* menu (shown below) which is found at the top of the Organizational Tree tab.



To update the Organizational Tree from the Management Server:

From the *Organizational Tree Update* menu, click **Refresh Tree**. The Tree is updated.

To update the Organizational Tree from the Directory:

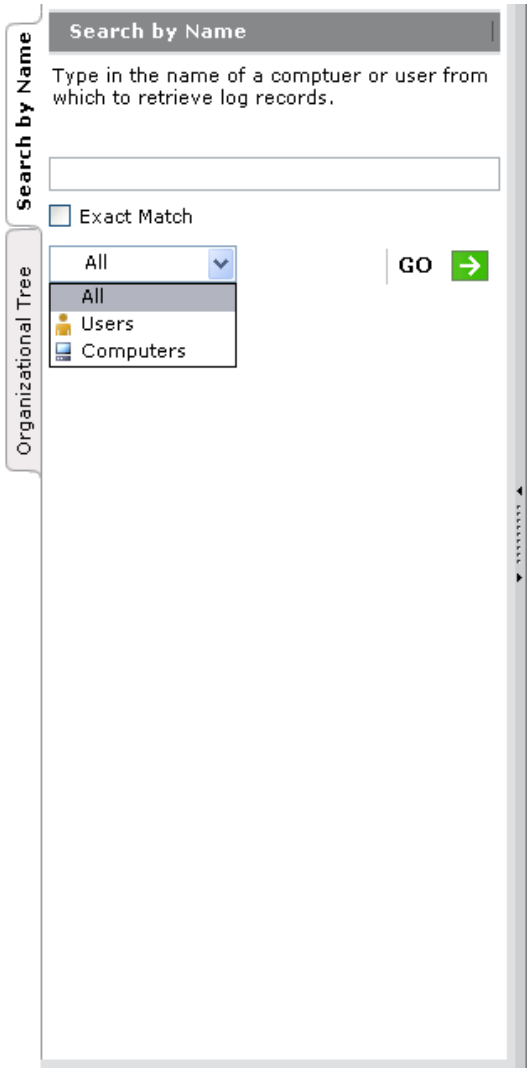
From the *Organizational Tree Update* menu (see previous figure), click **Sync Tree with Directory**. The Tree is updated, but this may take a while.

5.4.2 Filtering by Name

The *Search by Name* tab is an additional tool that you can use to determine the computers or users whose log records the Client or File log will display. The search criteria you enter here, along with queries (see *Queries*), determine which records are displayed in the Log Table (see *The Log Table*). This section describes how to use this tab to determine the logs displayed in the Client or file Log Table.

As mentioned, this tab does not appear in the Server log window, since by definition Server logs do not apply to computers or users.

The following figure show the *Search by Name* tab:

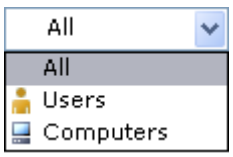


To search for specific computers or users:

1 In the text box, enter the name of the computer or user whose log record you wish to display in the Log Table. You may enter multiple names separated by comma, semicolon or space.

2 Check the **Exact Match** checkbox if you want the Log Table to display logs for a computer/user with the name that exactly matches the string you entered in the text box. For computers you must enter the full computer name (including the domain suffix). If **Exact Match** is not selected, the Log Table will contain logs for all computers and users whose name contains the string that you entered.

3 From the *Search by Name* menu



4 Select **Computer** if you want to search computer names, **User** if you want to search user names or **Any** if you want to search both computers and users.

5 Below the text box, click **GO** ( ). The logs now displayed in the log table originate from the computer/user (one or more) whose name matches your search criteria. If no computer or user is found whose name matches your search criteria the log table is empty.

5.5 Queries

Another method for filtering log records in the Log Table is the use of queries. You can define queries according to various criteria, or *properties*, so that only log records that match your specified criteria appear in the Log Table. In the case of Client logs and File logs, queries interact with your Organizational Tree selection to determine which records are displayed.

Three query types are available, covering the three available log types: Client Logs Queries, File Logs Queries and Server Logs Queries.

Queries may be defined and edited on an ad-hoc basis, or saved for future use. The default query is All Logs, which displays all the log records (to be exact – those that match your Organizational Tree selection criteria).

Once you have defined and saved a query, you can select it for use from the **Queries** menu in the toolbar

.

5.5.1 Built-in Queries

SafeGuard PortProtector comes with several built-in queries which you may use to start you off, if you wish. These include the following Client Logs Queries and File Logs Queries (no built-in queries are provided for Server Logs):

Built-in Client Logs Queries

- (**Built-in**) **All Alerts:** displays all Client Alerts, not including file alerts.
- (**Built-in**) **Blocked Devices:** displays all logs relating to blocking non-storage devices.
- (**Built-in**) **Blocked Storage Devices:** displays all logs relating to blocking storage devices.
- (**Built-in**) **Internal Port Events:** displays all logs relating to internal log events.
- (**Built-in**) **Suspension Events:** displays all administration events relating to Client suspension.
- (Built-in) Tampering Events: displays all tampering attempts.
- (**Built-in**) **WiFi Events:** displays all logs relating to WiFi events.

Built-in File Logs Queries

- (Built-in) All File Alerts: displays all File alerts.
- (**Built-in**) **Blocked Read Files:** displays all logs relating to blocked files read from storage devices.
- (**Built-in**) **Blocked Written Files:** displays all logs relating to blocked files written to storage devices.

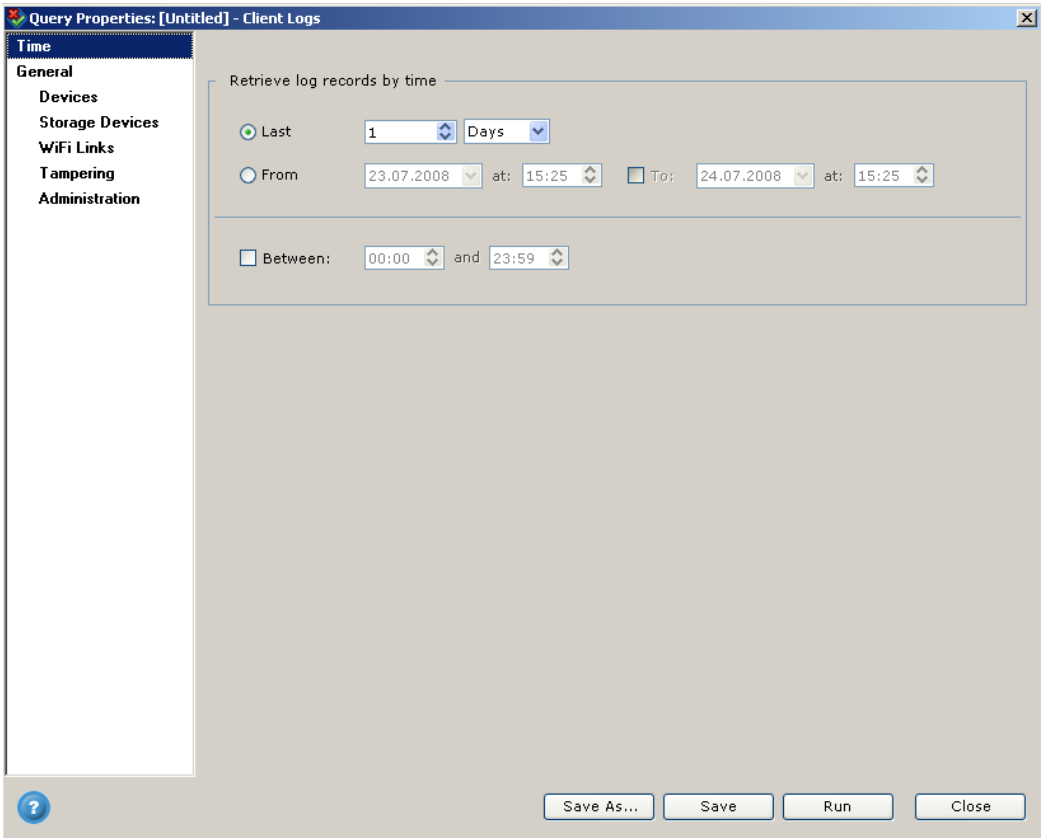
- **(Built-in) Offline Events:** displays all logs relating to file events that took place when an encrypted removable storage device was used by an authorized end-user on a non-company computer.
- **(Built-in) Sensitive Content Inspection Results:** displays all file events relating to sensitive content (use this only if you have activated Content Inspection).

5.5.2 Defining a New Client Log Query

Queries are defined in the *Query Properties* window. A different window is available for each log type (Client, Server or File logs). This section discusses Client Log queries. To learn how to define File Log queries, refer to *Defining a New File Log Query*. To learn how to define Server Log queries, refer to *Defining a New Server Log Query*.

To open the Query Properties window:

In the toolbar, click the **New Query** button . The *Query Properties* window opens:



Alternatively, you can open this window from the *Manage Queries* window (see *Managing Queries*).

The *Query Properties* window (see previous figure) is divided into two sections:

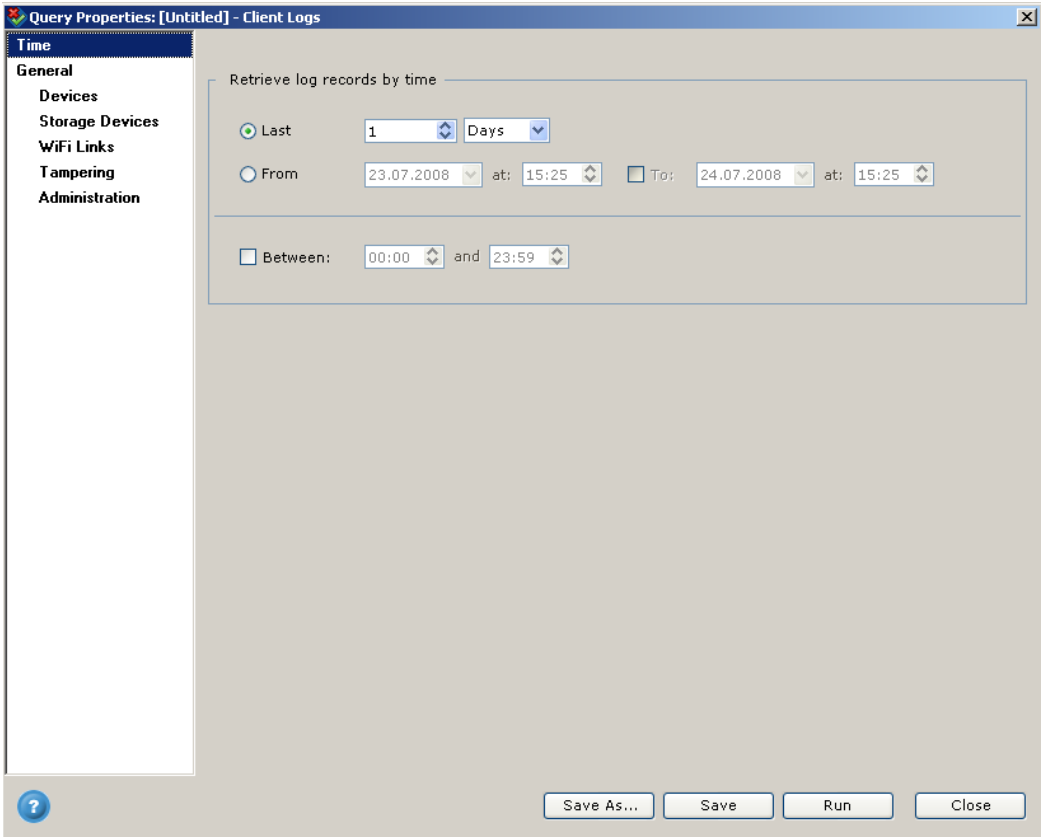
- **The left-hand section** lists the names of the various tabs in which you define the query properties. There are two main tabs, *Time* and *General*. Depending on the log type, additional tabs are available which include detailed definitions for topics that appear in the *General* window.

- **The right-hand section** displays the *Query Properties* tab that contains the corresponding definitions for the selection in the left-hand section. The definitions you make in these tabs form the criteria for deciding which records will be displayed in the Log Table; records must match the defined criteria.

We will now go over the various definitions and explain how they work.

5.5.2.1 Time Properties – Client Logs

Time query properties are defined in the *Time* tab, shown below:



5.5.2.1.1 Defining Time Properties – Client Logs

The **Time** tab is where you define the time frame for the records you wish to display. Regardless of other query definitions, the records in the Log Table will match the time criteria you set here.

To define time properties:

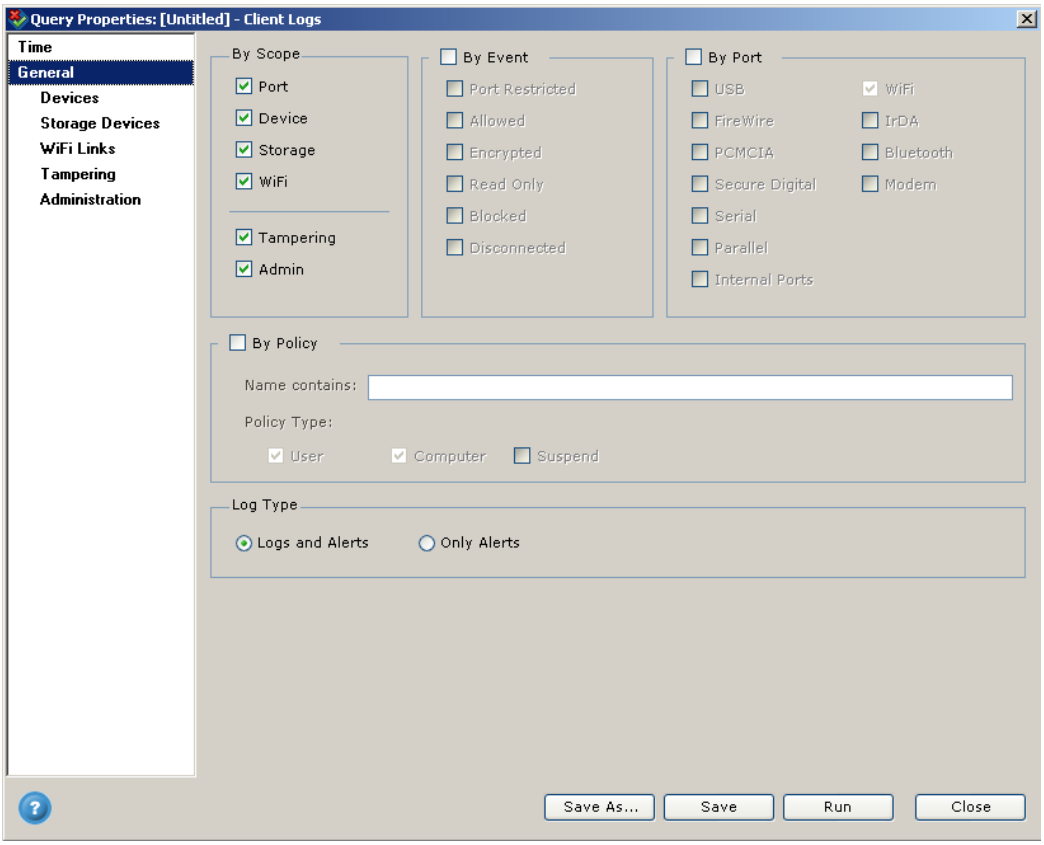
In the **Time** tab, enter the desired time frame for log records. Two options are available:

- Click the **Last** radio button to select a time period relative to the present day. If you wish, add a time window for the days in the selected period by checking the **Between** checkbox.
- Click the **From** radio button to select a definitive date and time from which to begin displaying records. Use the **To** checkbox if you want to set a definitive end time, so that only records falling between the **From** time and **To** time are displayed.

As a result, only records matching your selection will appear in the Log Table.

5.5.2.2 General Query Properties – Client Logs

General query properties are defined in this tab, shown below:



5.5.2.2.1 Defining General Query Properties – Client Logs

The **General** tab is where you define which log records will appear in the Log Table in terms of their, scope, port, event and additional properties. Only records matching the criteria you set here will appear in the Log Table.

The following describes the sections in this tab:

- **By Scope** – in this section you can select the scope you want Log Table to cover (you may select more than one type). If you select none, records will be displayed regardless of the scope to which they apply.

Note: You can define specific properties relating to each scope type. Port properties are defined in the By Port section in the General tab. Properties relating to the other scope types are defined in the other tabs named accordingly (device properties are defined in the Devices tab, storage device properties are defined in the Storage Devices tab etc.).

- **By Event** – in this section, you can select the event you want Log Table to cover (you may select more than one event). If you select none, records will be displayed regardless of the type of event to which they apply.

Note: Only event types relevant to your By Scope selection are available in this section. This means that if you select all scope types, all By Event options are enabled. However if, for example, you select scope type Port only, then only the Port Restricted and Blocked event options are enabled.

Note: If you select only Tampering and/or Administration in By Scope, the By Event section is disabled, as it is irrelevant for these scope types.

- **By Port** – in this section you can select the port you want the Log Table to cover (you may select more than one port). If you do not select this section, records will be displayed regardless of the type of port to which they apply.

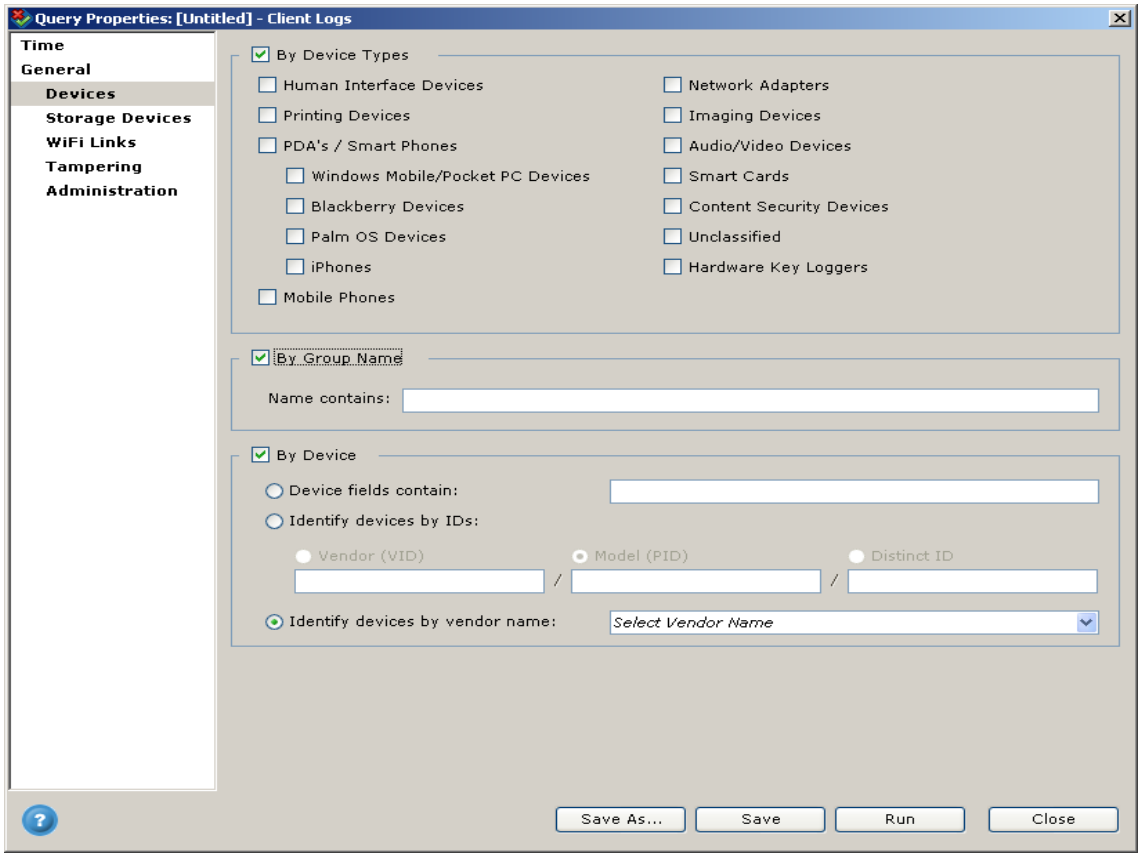
Note: Only ports relevant to your By Scope selection are available in this section. This means that if you select all scope types, all By Port options are enabled. However if, for example, you select Scope Storage only, then only the USB, FireWire and PCMCIA port options are enabled.

Note: If you select only Tampering and/or Administration in By Scope, the By Port section is disabled, as it is irrelevant for these scope types.

- **By Policy** - in this section you can enter the name (whole or partial) of the policy or policies you want Log Table records to be associated with. Only policies whose name contains the text you enter will be displayed. If you do select this section, the Log Table will display records regardless of the policy with which they are associated.
  If you select this section, you must select one of the policy types.
- **Log Type** – in this section you can select whether you wish to display both Log and Alert records, or only Alerts.

5.5.2.3 Device Properties – Client Logs

Device query properties are defined in the *Devices* tab, shown below:



5.5.2.3.1 Defining Device Query Properties – Client Logs

The **Devices** tab is where you define log records you wish to display in terms of their device attributes. Only records matching the criteria you set here will be displayed.

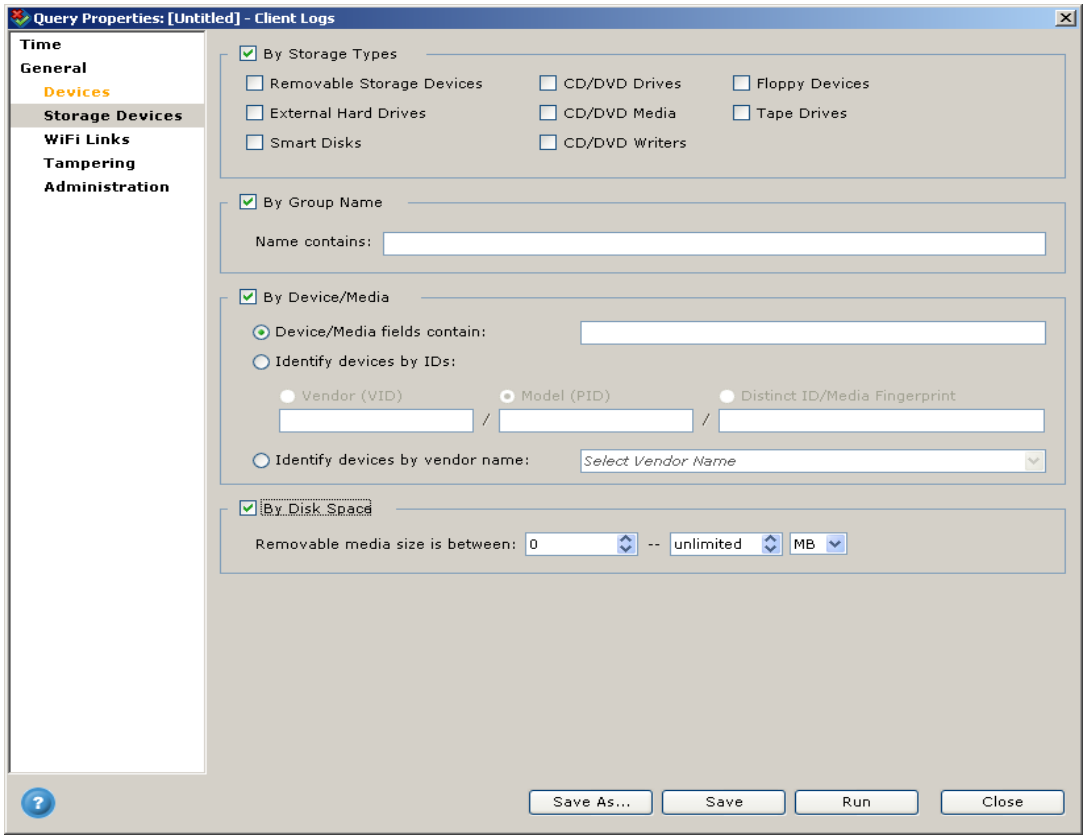
Note: This tab is enabled only if you select Device in the Scope section of the General tab.

The following describes the sections in this tab:

- **By Device Types** - in this section you can select the device type you want Log Table to cover (you may select more than one type). If you do not select this section, records will be displayed regardless of the type of device to which they apply.
- **By Group Name** - in this section you can enter the name (whole or partial) of the device group you want the Log Table to cover. Only devices belonging to these groups will be displayed. If you do not enter a group name, the Log Table will display records regardless of the group to which they belong.
- **By Device** – in this section you can select the devices you want the Log Table to cover. You may select them by entering the device name (whole or partial), or, alternatively, by their vendor ID, model or distinct ID. Alternatively, you may also identify devices by vendor name. If you make no selection in this section, records for all devices will be displayed.

5.5.2.4 Storage Device Properties – Client Logs

Storage Device query properties are defined in the *Storage Devices* tab, shown below:



5.5.2.4.1 Defining Storage Device Properties – Client Logs

The **Storage Devices** tab is where you define the log records you wish to display in terms of their storage device attributes. Only records matching the criteria you set here will appear in the Log Table.

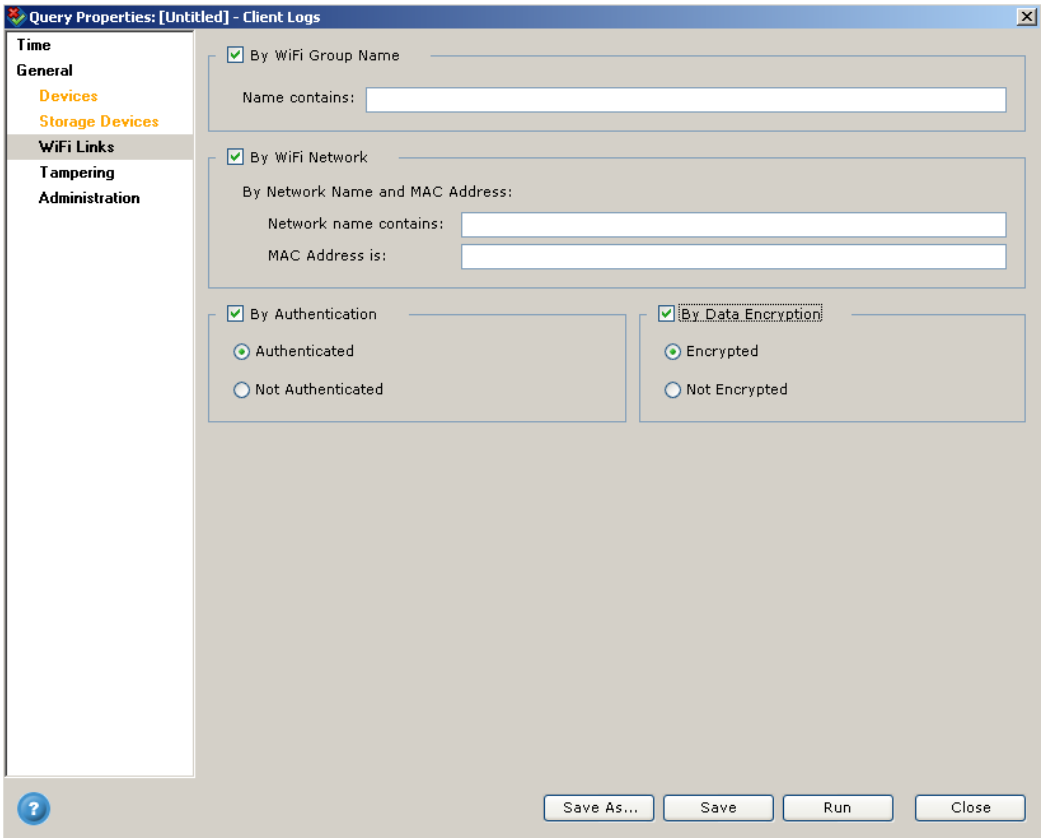
Note: This tab is enabled only if you select **Storage,** or make no selection (which is the same as selecting all), in the **Scope** section of the **General** tab.

The following describes the sections in this tab:

- **By Storage Types** - in this section you can select the storage device type you want the Log Table to cover (you may select more than one type). If you do not select this section, records will be displayed regardless of the type of storage device to which they apply.
- **By Group Name** - in this section you can enter the name (whole or partial) of the storage device group you want the Log Table to cover. Only devices belonging to these groups will be displayed. If you do not enter a group name, the Log Table will display records regardless of the group to which they belong.
- **By Device/Media** - in this section you can select the storage devices you want the Log Table to cover. You may select them by entering text from the device or CD/DVD medium name or other textual field (whole or partial), or, alternatively, by their vendor ID, model or distinct ID, or in the case of CD/DVD media their fingerprint. Alternatively, you may also identify devices by vendor name. If you make no selection in this section, records for all devices which belong to the Storage Types you select will be displayed.
- **By Disk Space** – if you select By Storage Type (see above) **Removable Storage Devices** or **External Hard Disks**, this section allows you to define the media size range which the Log Table should cover. If you select none, the Log Table will display records for storage devices regardless of their space size.

5.5.2.5 WiFi Connection Properties – Client Logs

WiFi connection query properties are defined in the *WiFi* links tab, shown below:



5.5.2.5.1 Defining WiFi Connection Properties – Client Logs

The **WiFi Links** tab is where you define the log records you wish to display in terms of their WiFi attributes. Only records matching the criteria you set here will appear in the Log Table.

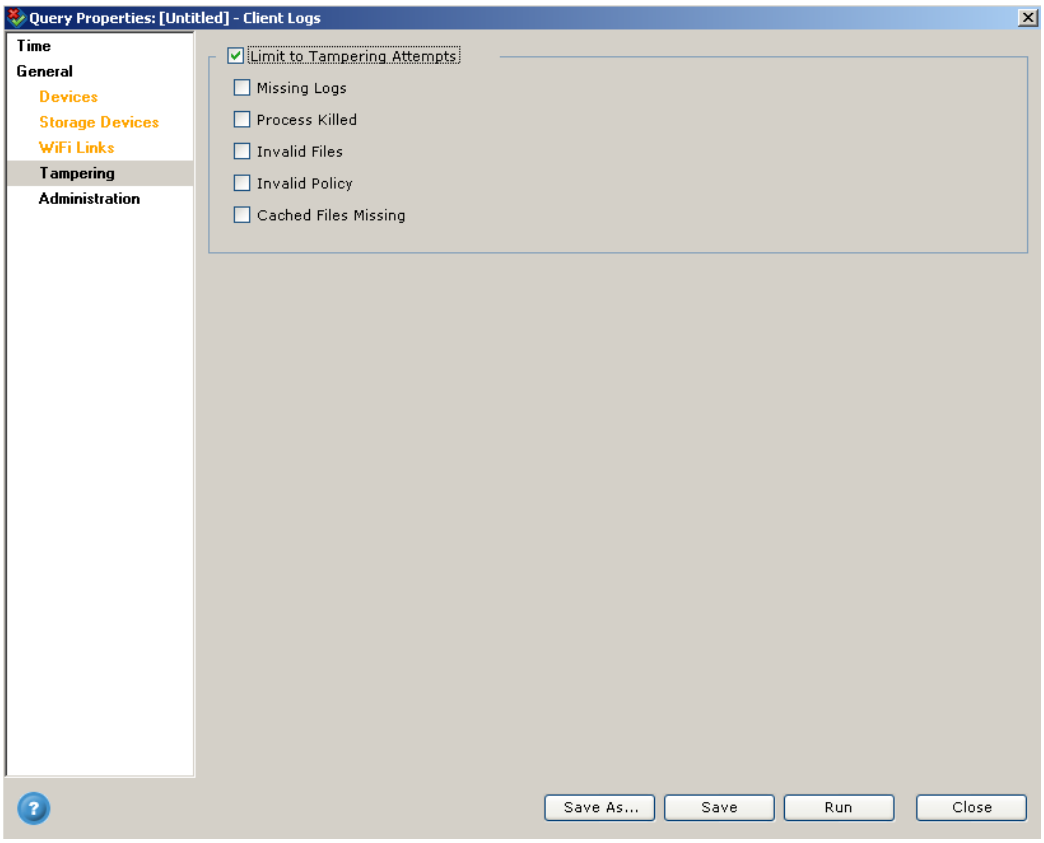
Note: This tab is enabled only if you select **WiFi,** in the **Scope** section of the **General** tab.

The following describes the sections in this tab:

- **By WiFi Group Name** - in this section you can enter the name (whole or partial) of the WiFi group you want the Log Table to cover. Only log records associated with the WiFi connections belonging to these groups will be displayed. If you do not enter a group name, the Log Table will display records regardless of the group to which they belong.
- **By WiFi Network** - in this section you can enter the name (whole or partial) of the network you want the Log Table to cover, and/or its MAC address. Only log records with the selected network properties will be displayed. If you do not enter network properties, the Log Table will display records regardless of the network with which they are associated.
- **By Authentication** - in this section you can determine whether the WiFi links in the Log Table should be authenticated connections. Instead, we can say that if you want the log records for both authenticated and not authenticated, don't select this section.
- **By Data Encryption** - in this section you can determine whether the WiFi connections in the Log Table should be encrypted connections or not.

5.5.2.6 Tampering Properties – Client Logs

Tampering query properties are defined in the *Tampering* tab, shown below:



5.5.2.6.1 Defining Tampering Properties – Client Logs

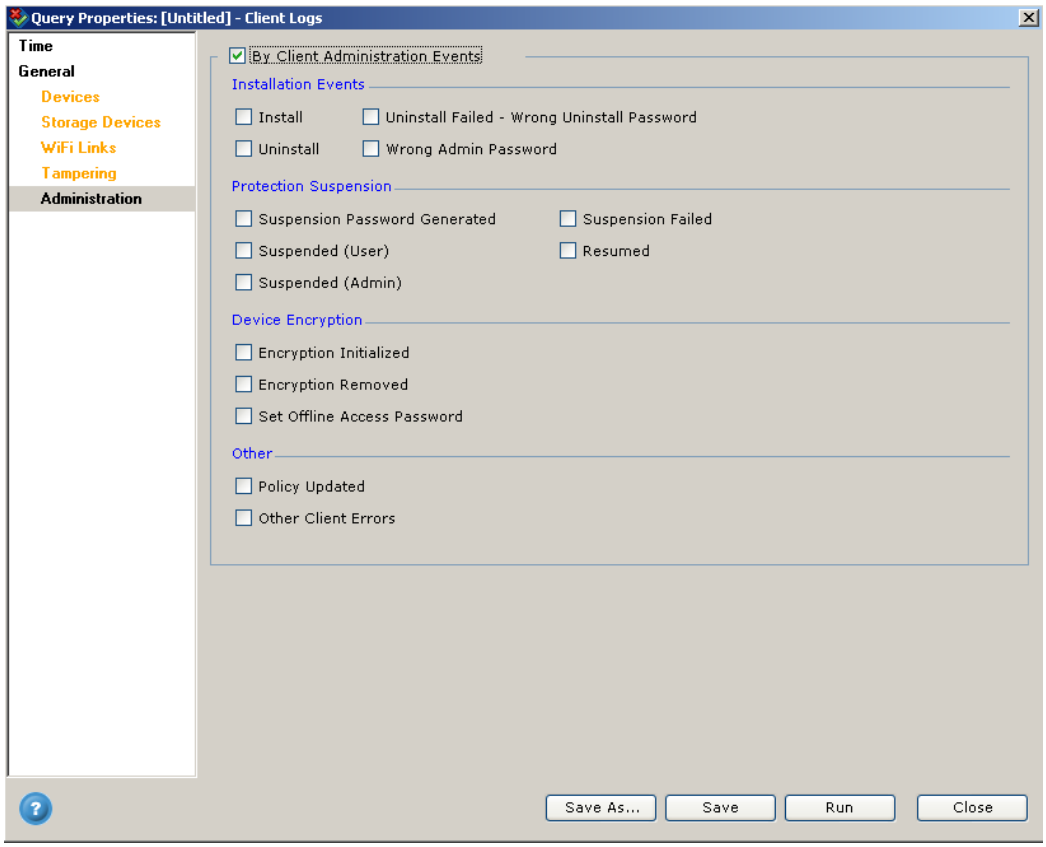
The **Tampering** tab is where you define the log records you wish to display in terms of their tampering attempt event. Only records matching the criteria you set here will appear in the Log Table.

Note: This tab is enabled only if you select **Tampering**, in the **Scope** section of the **General** tab.

In the Limit to Tampering Attempts section you can select the type of attempt you want Log Table to cover (you may select more than one event). If you do not select this section, records will be displayed regardless of the type of tampering attempt to which they apply.

5.5.2.7 Administration Properties – Client Logs

Administration query properties are defined in the *Administration* tab, shown below:



5.5.2.7.1 Defining Administration Properties – Client Logs

The **Administration** tab is where you define the log records you wish to display in terms of their administration events. Only records matching the criteria you set here will appear in the Log Table.

Note: This tab is enabled only if you select **Administration**, in the **Scope** section of the **General** tab.

By Client Administration Events – check this checkbox to select the Client administration events you want the Log Table to cover. The events are arranged in groups. You may select events from different groups, and in each group you may select more than one event.

If you do not select this section, log records will be displayed regardless of the Client administration event to which they apply.

The following describes the groups available in this tab:

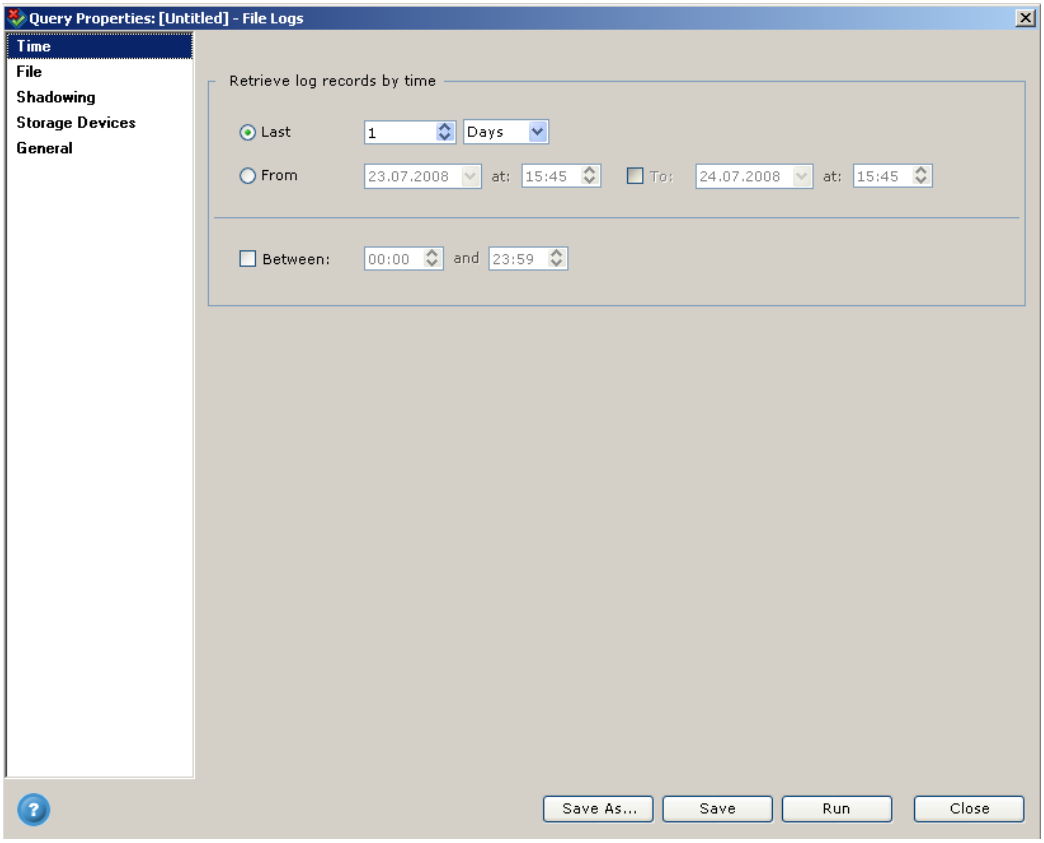
- **Installation Events** - in this group you can select the installation events to be covered by the Log Table.
- **Protection Suspension** - in this group you can select the protection suspension events to be covered by the Log Table.
- **Device Encryption –** in this group you can select the device encryption events to be covered by the Log Table.
- **Other** – in this group, click the checkboxes to display records which apply to policy updating or to other Client errors.

Note: The selections in the Administration tab interact with each other using a Boolean "OR", meaning records that meet any of the criteria you set in this tab will be displayed in the Log Table.

5.5.3 Defining a New File Log Query

File Log queries allow you to filter the Log Table according to various properties. They contain the following tabs: Time, File Shadowing, Storage Devices and General. Time Properties – File Logs

Time query properties are defined in the *Time* tab, shown below:



5.5.3.1.1 Defining Time Properties – File Logs

The **Time** tab is where you define the time frame for the records you wish to display. Regardless of other query definitions, the records in the Log Table will match the time criteria you set here.

To define time properties:

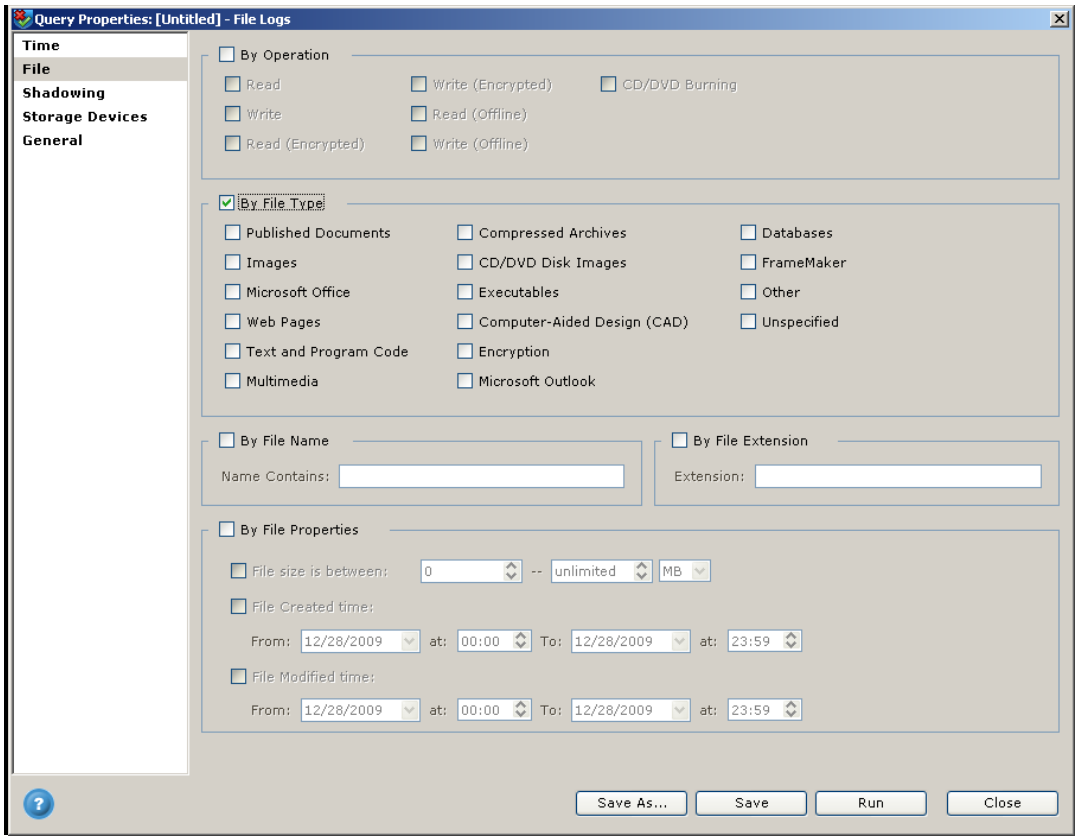
In the **Time** tab, enter the desired time frame for log records. Two options are available:

- Click the Last radio button to select a time period relative to the present day. If you wish, add a time window for the days in the selected period by checking the Between checkbox.
- Click the From radio button to select a definitive date and time from which to begin displaying records. Use the To checkbox if you want to set a definitive end time, so that only records falling between the From time and To time are displayed.

As a result, only records matching your selection will appear in the Log Table.

5.5.3.2 File Properties – File Logs

Query file properties are defined in the *File* tab, shown below:



5.5.3.2.1 Defining File Properties – File Logs

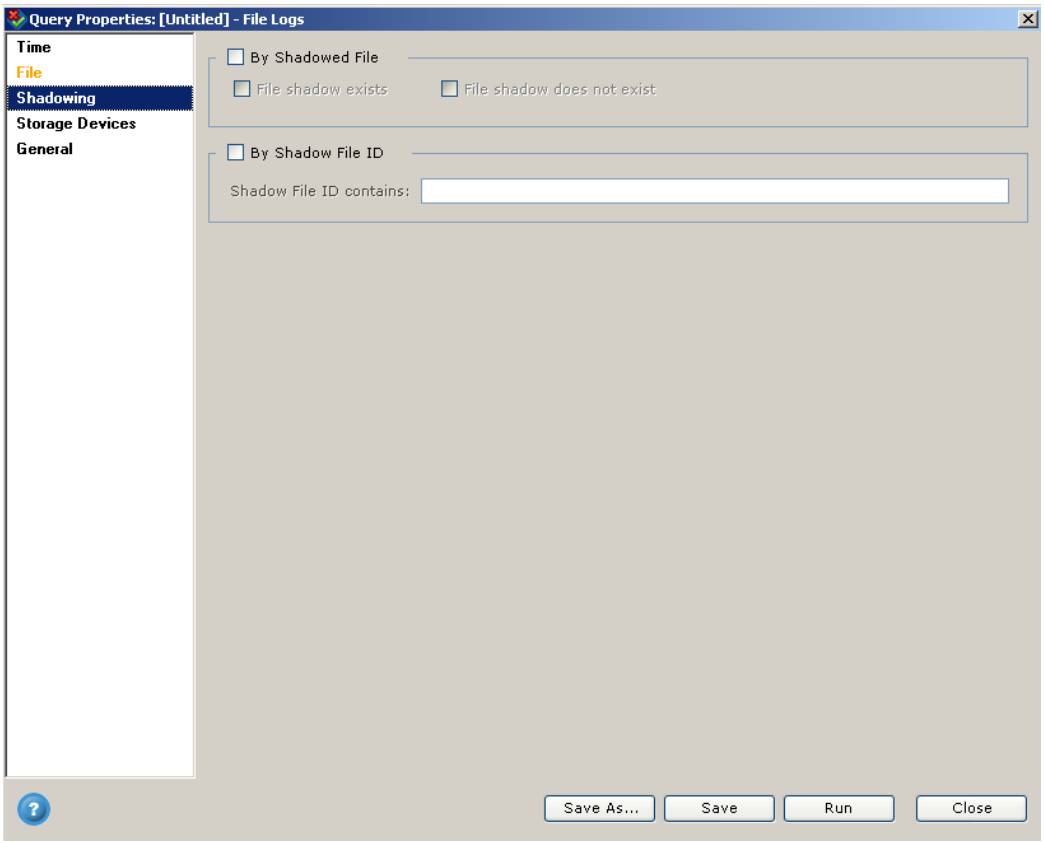
The **File** tab is where you define the log records you wish to display in terms of their file attributes. Only records matching the criteria you set here will appear in the Log Table.

The following describes the sections in this tab:

- **By Operation** – check this checkbox if you want the Log Table to display logs for files read from devices, files written to devices, files read from encrypted devices or files written to encrypted devices. Then, select the appropriate checkbox for the required operation (you may select more than one option). If you leave the **By Operation** checkbox unchecked, logs for all operations will be included in the Log Table.
- **By File Type** – check this checkbox if you want the Log Table to display logs for specific file types only. Then, select the appropriate checkbox for the required type (you may select more than one option). If you leave the **By File Type** checkbox unchecked, logs for all file types will be included in the Log Table.
- **By File Name** – check this checkbox if you want the log table to include logs only for files whose name contains a specified string. Enter that string in the **Name Contains** field.
- **By File Extension** - check this checkbox if you want the Log Table to include logs only for files of a certain type, by their extension. Then, enter the file extension in the **Extension** field. You may enter more than one extension, in which case extensions should be separated by a semicolon or a colon.
- **By File Properties** - click this checkbox if you want the log table to include logs only for files that have the properties specified in this section – **File Size**, **File Created** time or **File Modified** time. Check the desired checkbox for each of these properties, then set the required parameters as needed.

5.5.3.3 Shadowing Properties – File Logs

The **Shadowing** tab enables you to define query properties regarding shadowed files, as shown below:



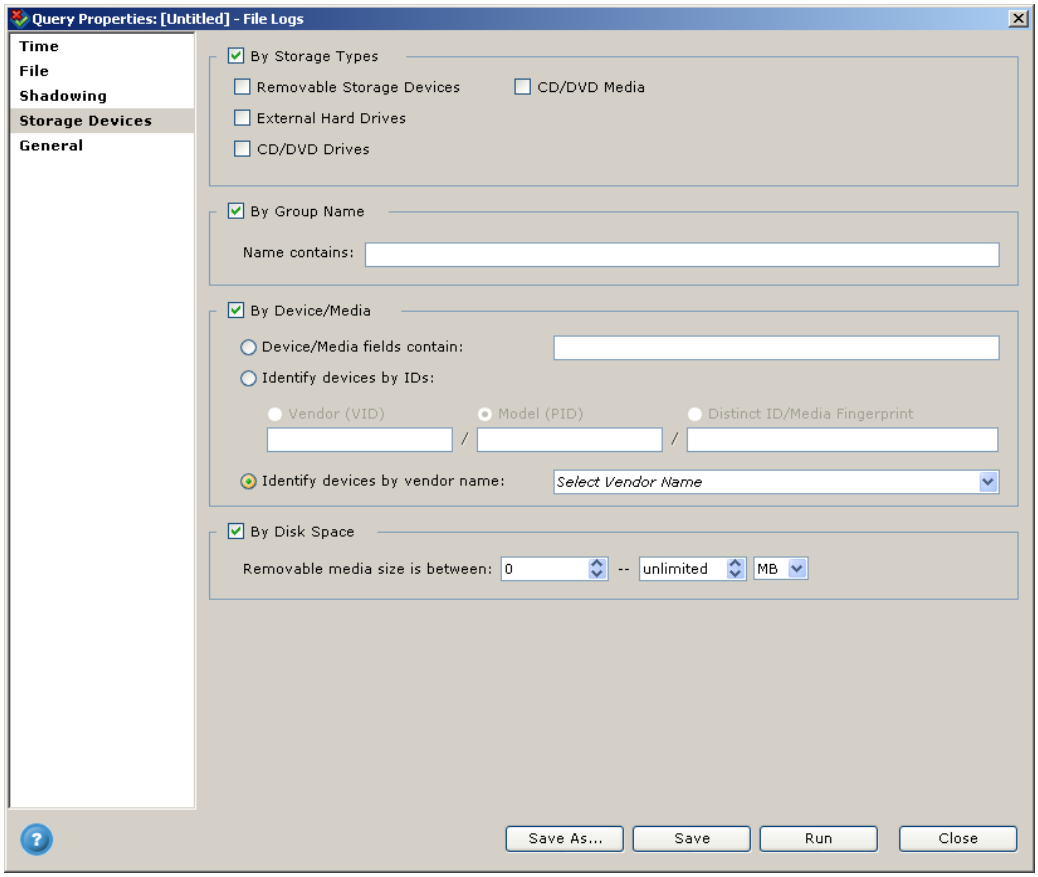
5.5.3.3.1 Defining File Shadowing Properties – File Logs

The following describes the sections in this tab:

- **By Shadowed File** - in this section you specify that the log files listed in the query results are dependent upon whether a shadowed file copy was made of the logged file or not.
- Check the **Shadow File Exists** checkbox to specify that the log files in the query's results include the logs of files that were shadowed. These logs show the actual files that were copied.
- Check the **No Shadow File Exists** checkbox to specify that the log files in the query's results include the logs of files that were not shadowed.
- **By File ID** - in this section you specify the precise ID of the shadowed file to be shown in the query results. In the **Shadow File ID contains** field specify all or part of the Log File ID. This Log File ID may be included in an alert message that was sent when the file was shadowed.

5.5.3.4 Storage Device Properties – File Logs

Query Storage Device properties are defined in the *Storage Devices* tab, shown below:



5.5.3.4.1 Defining Storage Device Properties – File Logs

The **Storage Devices** tab is where you define the log records you wish to display in terms of their storage device attributes. Only records matching the criteria you set here will appear in the Log Table.

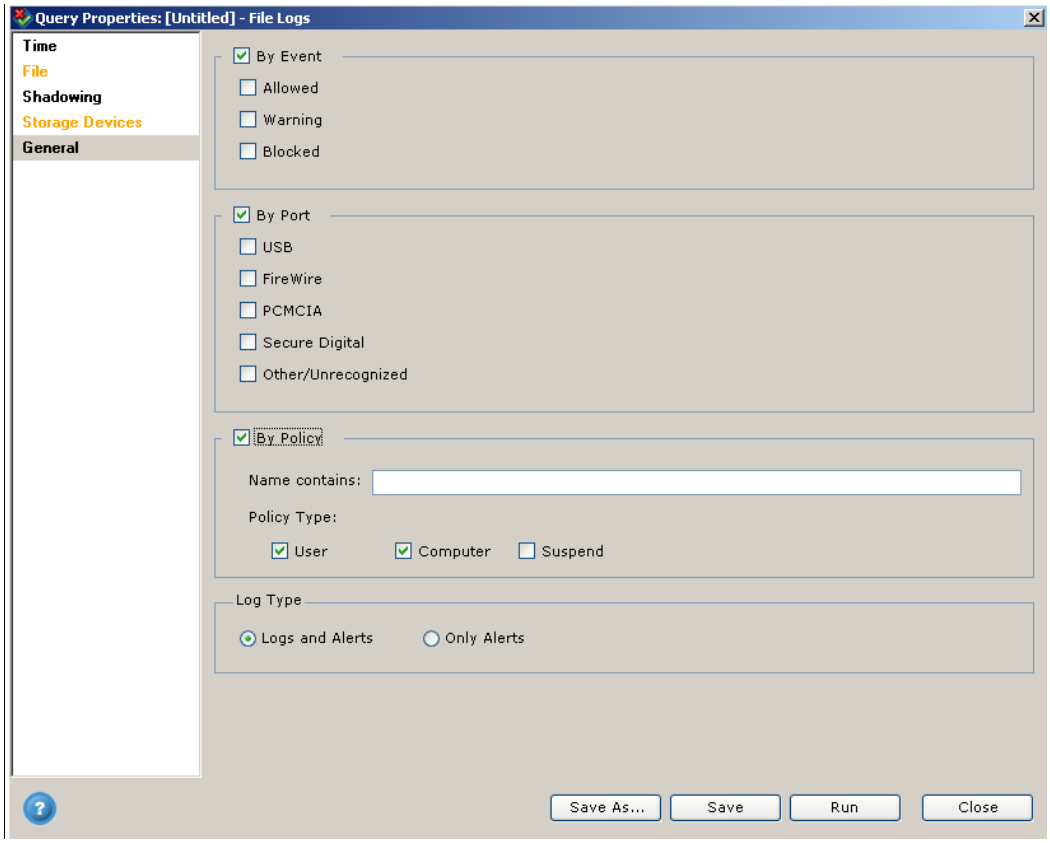
The following describes the sections in this tab:

- **By Storage Types** - in this section you can select the storage device type (including CD/DVD media) you want the Log Table to cover (you may select more than one type). If you do not select this section, records will be displayed regardless of the type of storage device to which they apply.
- **By Group Name** - in this section you can enter the name (whole or partial) of the storage device group you want the Log Table to cover. Only devices belonging to these groups will be displayed. If you do not enter a group name, the Log Table will display records regardless of the group to which they belong.
- **By Device/Media** - in this section you can select the storage devices or CD/DVD media you want the Log Table to cover. You may select them by entering the device name (whole or partial) or other textual field or, alternatively, by their vendor ID, model or distinct ID, or fingerprint in the case of CD/DVD media. Alternatively, you may also identify storage devices by vendor name. If you make no selection in this section, records for all devices which belong to the Storage Types you select will be displayed.

- **By Disk Space** – if you select By Storage Type (see above) **Removable Storage Devices** or **External Hard Disks**, this section allows you to define the media size range which the Log Table should cover. If you select none, the Log Table will display records for storage devices regardless of their space size.

5.5.3.5 General Properties – File Logs

General query properties are defined in the *General* tab, shown below:



5.5.3.5.1 Defining General Properties – File Logs

The **General** tab is where you define the log records you wish to display in terms of their port and policy attributes. Only records matching the criteria you set here will appear in the Log Table. The following describes the sections in this tab:

- **By Event** – check this checkbox if you want the log to display only files associates with a specific file control event. In this case, select the appropriate Checkbox for those events you want to include.
- **By Port** – check this checkbox if you want the log to display only files associates with specific ports. In this case, select the appropriate Checkbox for those ports you want to include.
- **By Policy** - in this section you can enter the name (whole or partial) of the policy or policies you want Log Table records to be associated with. Only policies whose name contains the text you enter will be displayed. If you do select this section, the Log Table will display records regardless of the policy with which they are associated.
  If you select this section, you must select one of the policy types.

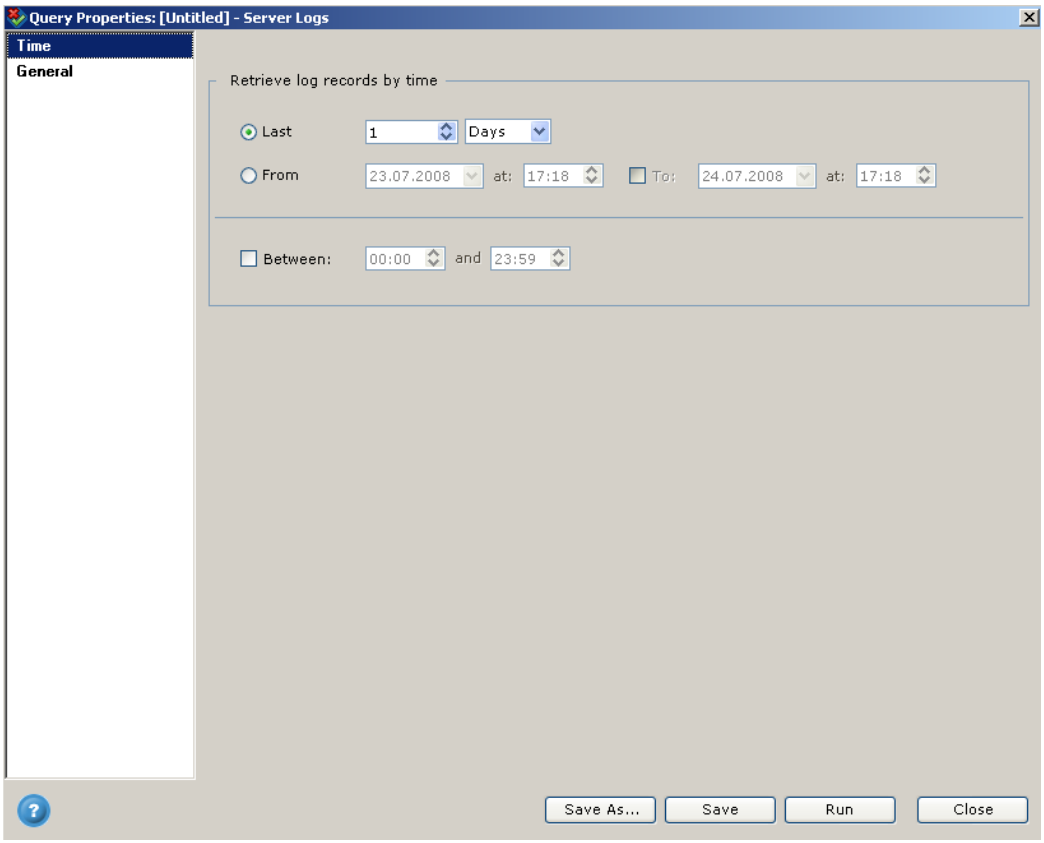
- **Log Type** – in this section, select whether you would like the Log table to display both logs and alerts, or only alerts (depending on the way you defined log and alert settings in your policies' *File Control* window, displaying both logs and alerts may produce a very large number of records). Click the desired radio button.

5.5.4 Defining a New Server Log Query

Server Log queries allow you to filter the Management Server Log Table according to various properties relevant to Server events. They contain the Time and General tabs.

5.5.4.1 Time Properties – Server Logs

Time query properties are defined in the *Time* tab, shown below:



5.5.4.1.1 Defining Time Properties – Server Logs

The **Time** tab is where you define the time frame for the records you wish to display. Regardless of other query definitions, the records in the Log Table will match the time criteria you set here.

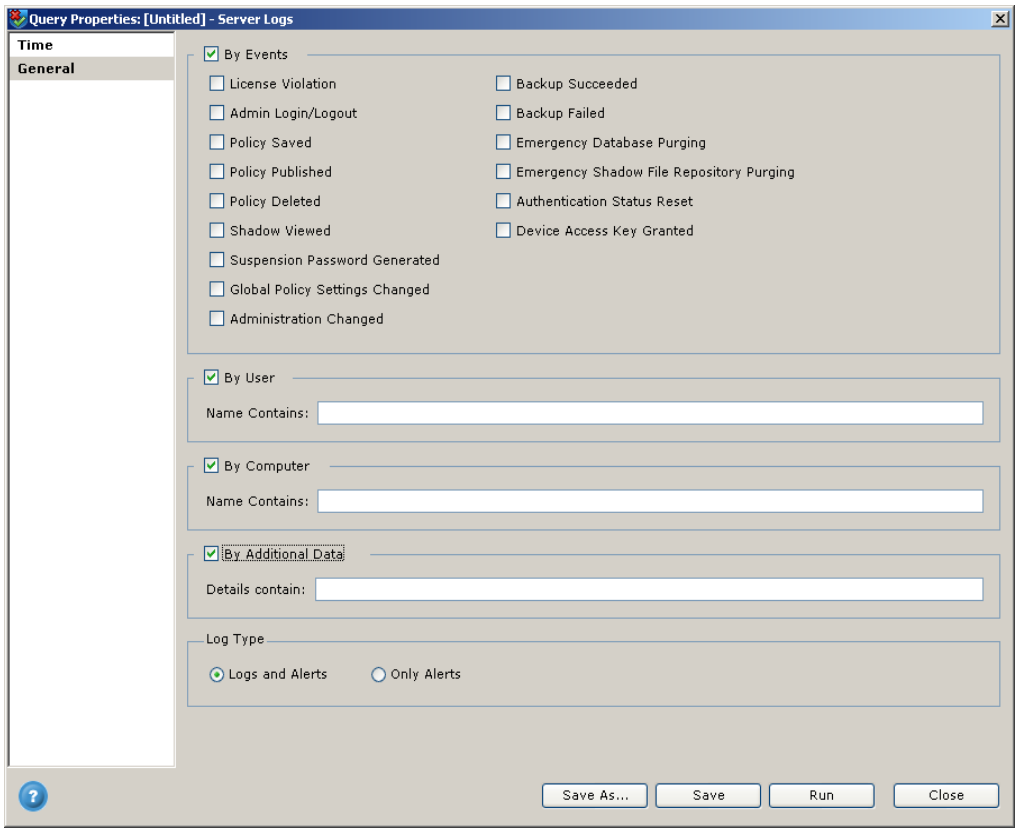
To define time properties:

In the **Time** tab, enter the desired time frame for log records. Two options are available:

- Click the **Last** radio button to select a time period relative to the present day. If you wish, add a time window for the days in the selected period by checking the **Between** checkbox.
- Click the **From** radio button to select a definitive date and time from which to begin displaying records. Use the **To** checkbox if you want to set a definitive end time, so that only records falling between the **From** time and **To** time are displayed. As a result, only records matching your selection will appear in the Log Table.

5.5.4.2 General Properties – Server Logs

General query properties are defined in the *General* tab, shown below:



5.5.4.2.1 Defining General Properties – Server Logs

The **General** tab is where you define the log records you wish to display in terms of their attributes. Only records matching the criteria you set here will appear in the Log Table.

The following describes the sections in this tab:

- **By Events** – click this checkbox if you want the log to display records that pertain to specific Server events. Select the required events by checking the appropriate checkbox.
- **By User** - click this checkbox if you want the log table to include records that pertain to a specific administrator whose name contains a specific string. In this case, enter the required string in the Name Contains field.
- **By Computer** - click this checkbox if you want the log table to include records that pertain to a specific SafeGuard PortProtector Management Console whose name contains a specific string. In this case, enter the required string in the Name Contains field.
- **By Additional Data** - click this checkbox if you want the log table to include records that contain certain string in their Details field. In this case, enter the required string in the **Details Contain** field.
- **Log Type** – in this section, select whether you would like the Log table to display both logs and alerts, or only alerts.

5.5.5 Running a New Query

If you wish, you can run a new query immediately from within the *Query Properties* window.

To run a new query:

In the *Query Properties* window, after saving the query click **Run**. The query is activated and the Log Table displays records matching your query criteria.

Note: If you do not save and name the new query before running it, it will not be available for future use once it is no longer the active query.

5.5.6 Saving a New Query

Once you have completed the query definition, you can save the query for repeated use in the future.

To save a new query:

1 In the *Query Properties* window, click **Save**. A *Save Query* window opens.

2 In the *Save Query* window, enter the desired Query Name (mandatory) and its description (optional), and click **OK**. The query is saved, and from now on can be selected from the Query toolbar menu.

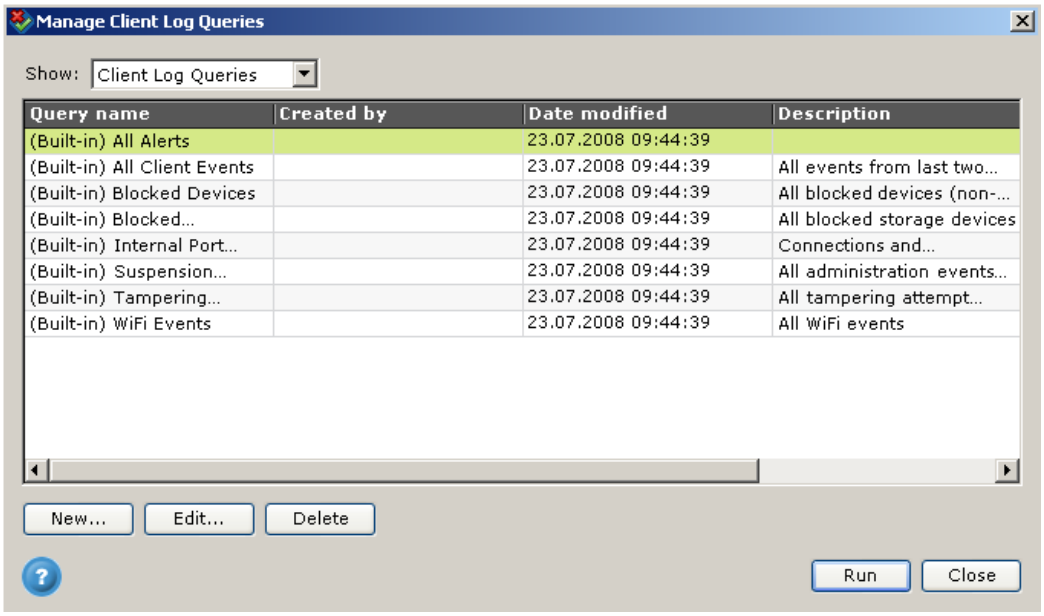
5.5.7 Managing Queries

To open the Manage Queries window:

From the toolbar, click the **Manage Queries** button .

OR

In the *File* menu, click **Queries**. The *Manage Queries* window opens:



5.5.7.1 Query Management Options

The *Manage Queries* window displays the built-in queries (described in *Built-in Queries*) as well as your saved queries for selected query type (Client logs, File logs or Server logs). In this window you can perform the following activities:

- Define new queries, explained in *Creating a Query*.
- Edit existing queries, explained in *Editing a Query*.
- Delete queries, explained in *Deleting a Query*.
- Rename queries, explained in *Renaming a Query*.
- Run queries, explained in *Running a Previously Defined Query*.

As a default, this window lists all queries for the active log type (Client log, Server log or File log). If you wish, you can show and manage queries for a different log type.

To change query log type:

In the Manage Queries window, click the Show menu and select the required log type for the queries you want to manage. The window now lists queries for the log type you selected.

5.5.7.2 Creating a Query

The process of creating a new query is explained in detail in *Queries*. The *Query Properties* window, in which you define the new query's properties, can also be opened from the *Manage Queries* window.

5.5.7.3 Editing a Query

A query may be edited when there is a need to change its properties, or when you want to use it as a template for creating a new query.

To edit a query:

1 From the toolbar, click the **edit** button . The *Query Properties* window opens.

2 Make the desired changes.

OR

1 In the *Manage Queries* window, select the query you wish to edit from the query list.

2 Click **Edit**. The *Query Properties* window opens.

3 Make the desired changes.

OR

1 In the Manage Queries window, from the query list, right-click the query you wish to edit.

2 From the right-click menu, select **Edit**. The *Query Properties* window opens.

3 Make the desired changes.

To save an edited query:

1 Saving a query with its existing name:

2 Click **Save** to save the modified query with its existing name.

3 Saving the modified query as a new query:

4 Click **Save As**. A *Save Query* window opens.

5 In the *Save Query* window, enter the desired Query Name (mandatory) and its description (optional), and click **OK**. The query is saved, and from now on can be selected from the Query toolbar menu.

5.5.7.4 Deleting a Query

You may delete queries for which you no longer have use.

To delete a query:

1 In the *Manage Queries* window, select the query you wish to delete from the query list (you may use **Ctrl** and **Shift** to select more than one query to delete).

2 Click **Delete.** A verification window opens.

3 Click **Yes** to delete the query(s), or **No** to cancel.

OR

1 From the query list, right-click the query you wish to delete (before you right-click, you may use **Ctrl** and **Shift** to select more than one query to delete).

2 From the right-click menu, click **Delete**. A verification window opens.

3 Click **Yes** to delete the query(s), or **No** to cancel.

5.5.7.5 Renaming a Query

1 In the *Manage Queries* window, select the query you wish to delete from the query list.

2 Click the **Name** field. Query Name is now selected and can be edited.

5.5.8 Running a Previously Defined Query

Running a query applies the query criteria as you have defined them. Along with the Organizational Tree selection, this determines which records appear in the Log Table. There are various ways in which you can run a previously defined query: from the toolbar, from the *Manage Queries* window using the **Run** button, from the *Manage Queries* window using the right-click menu or from the *Manage Queries* window by double-clicking the query.

To run a previously defined query from the toolbar:

In the toolbar, click the **Query** menu and select the query you wish to apply. The query is applied to the Log Table.

To run a previously defined query from the *Manage Queries* window:

1 In the *Manage Queries* window, select the query you wish to run from the query list.

2 Click **Run.** The query is applied to the Log Table.

OR

1 From the query list, right-click the query you wish to run.

2 From the right-click menu, click **Run**. The query is applied to the Log Table.

OR

From the query list, double-click the query you wish to run. The query is applied to the Log Table.

Note: If the query you run belongs to a different type than the active Log Table (for example, the active Log Table shows Client logs and the query applies to Server logs), a new, additional Log window opens displaying the new Log Table.

5.5.9 Discontinuing Query Application

If you wish to discontinue query application and to revert back to the default Log Table display – All Logs – you can do so by selecting All Logs in the *Queries* menu. The Log Table now displays All Logs.

5.6 Active Window Options

The active window can be duplicated, undocked and closed. These options are described in *Active Window Options* in *Chapter 2, Getting Started*.

5.7 Collecting Logs

This option enables you to collect logs from a served computer outside the scheduled collection times, in order to view its most recent information. Activating this function collects all log types. Refer to *Retrieving Latest Information from a Client* in *Chapter 6, Managing Clients* for instructions

5.8 Tracking Client Task Progress

When the application is in the process of performing tasks (such as collecting logs or updating policies), you may view the progress of these tasks. Refer to *Tracking Client Task Progress* in *Chapter 6, Managing Clients* for instructions.

5.9 Log Table Structures

The following describes the columns in the Log tables:

- Client Log Structure describes the columns in the Client Log table.
- File Log Structure describes the columns in the File Log table.
- Server Log Structure describes the columns in the Server Log table.

5.9.1 Client Log Structure

The following describes the columns in the Client Log table:

Column	Description
Log Type	This column specifies whether the record is a log or an alert.
Scope	This column specifies what scope the event applies to (e.g. Port, Storage, Admin, Tampering).
Time	This column displays the time of the event, in terms of Management Console time.
Computer	This column displays the full name (including the domain suffix) of the computer to whom the event applies.
User	This column displays the name of the user to whom the event applies.

Column	Description
Event	This column displays the event. Possible values are: • Port restricted • Allowed • Encrypted • Read Only • Blocked • Disconnected • Missing Logs (tampering attempt) • Process Killed (tampering attempt) • Invalid Files (tampering attempt) • Invalid Policy (tampering attempt) • Install • Uninstall • Uninstall Failed • Wrong Admin Password • Resumed (i.e. protection resumed following suspension) • Set Offline Access Password • Polciy Updated • Other Client Errors • Access Password Changed • Wrong Access Password • Not Authenticated Access
Port	This column displays the port type of the port associated with the event.
Device Type	This column displays the device type of the device associated with the event.

Column	Description
Device Description	This column displays the description of the device associated with the event. The device description is derived from the device.
Device Info	This column displays the device information of the device associated with the event. The device information is derived from the device.
Group	This column display the name of the group of approved devices, storage devices or WiFi connections, to which the device or connection associated with the event belongs.
Policy Type	This column specifies whether the applied policy is a computer policy or a user policy.
Policy	This column displays the name of the policy that is applied to the reporting Client. If policies are merged on this Client, all merged policies are listed.
Vendor	This column displays the device vendor.
Model	This column displays the device model.
Distinct ID	This column displays the device distinct ID, when available.
Details	This column displays additional information when necessary. E.g. encryption type (for WiFi network encryption), tampered file name etc.
Client Local	This column displays the event time in local time of the Client that reported this event.
DB Insert	This column displays the time the event was inserted into the database in terms of Management Console time.
Sequence	Each Client sends its logs with a sequence that helps detect missing logs and alerts about log tampering attempts. You can use this when a "Missing logs" event appears for a specific computer.

5.9.2 File Log Structure

The following describes the columns in the File Log table:

Column	Description
Log Type	This column specifies whether the record is a log or an alert.
Time	This column displays the time of the event, in terms of Management Console time.
Computer	This column displays the full name (including the domain suffix) of the computer to whom the event applies.
User	This column displays the name of the user to whom the event applies.
Event	This column displays the file event. Possible values are: • Allowed • Warning (when using Content Inspection and sensitive content is detected) • Blocked If you selected to block file writing when the burning format does not enable logging (see *Setting CD/DVD Permissions* in *Chapter 3, Defining Policies*) this column indicated that writing was blocked.
Operation	This column displays the type operation performed. Possible values are: • Read • Write • Read (encrypted) • Write (encrypted) • Read (offline) • Write (offline)
File Type	This column displays the name of the file type (e.g. Microsoft Word)

Column	Description
Extension	This column displays the extension of the logged file.
File Name	This column displays the path and name of the logged file.
Shadow File	This column displays a checkmark if a file was shadowed for this log entry.
Shadow File ID	This column displays the unique file ID of the shadowed file represented by this log entry in the file shadow repository. You may refer to *Step 14: Define File* Shadowing for information about configuring the file shadowing central repository.
File Size	This column displays the size of the logged file, in bytes.
Created	This column displays the date and time when the logged file was created.
Modified	This column displays the date and time when the logged file was modified.
Inspect Results	This column appears only when content inspection is performed and displays the inspection results. Possible values are: • Sensitive • OK • Failed • empty (not inspected)
Inspect Time	This column appears only when content inspection is performed and displays the date & time of inspection.
Inspect Details	This column appears only when content inspection is performed and the file content is found to be sensitive. The column displays details received from Websense-PortAuthority.
Port	This column displays the port associated with the file event.

Column	Description
Device Type	This column displays the device type of the device associated with the file event.
Device Description/ Network	This column displays the device description of the device/network associated with the file event.
Device Info	This column displays the device information of the device associated with the file event.
Group Name	This column display the name of the group of approved devices, storage devices or WiFi connections, to which the device or connection associated with the event belongs.
Policy Type	This column specifies whether the applied policy is a computer policy or a user policy.
Policy	This column displays the name of the policy that is applied to the reporting Client. If policies are merged on this Client, all merged policies are listed.
Vendor	This column displays the device vendor.
Model	This column displays the device model.
Distinct ID	This column displays the device distinct ID, when available.
Details	This column displays additional details when available.
Client Local	This column displays the event time, in terms of the time of the Client reporting the event.
DB Insert	This column displays the time the Management Server received this event, in terms of the Management Console time.

Column	Description
Sequence	Each Client sends its logs with a sequence that helps detect missing logs and alerts about log tampering attempts. You can use this when a "Missing logs" event appears for a specific computer.

5.9.3 Server Log Structure

The following describes the columns in the Server Log table:

Column	Description
Log Type	This column specifies whether the record is a log or an alert.
Scope	This column specifies what scope the event applies to (e.g. Admin, License).
DB Insert	This column displays the event time in terms of Management Console local time.
Computer	This column displays the name of the Management Console to whom the event applies.
User	This column displays the name of the administrator to whom the event applies.

Column	Description
Event	This column displays the event type. Possible values: • License • Admin Login/Logout • Policy Saved • Policy Published • Policy Deleted • Suspension Password Generated • Global Policy Settings Changed • Administration Changed • Backup Succeeded • Backup Failed • Emergency Database Purging
Details	This column displays additional details when available. E.g. license alert details, policy name in case of Policy Published event, etc.

5.10 Viewing Shadowed Files

File Shadowing provides the ability to track and collect copies of files that have been moved to/from external storage devices. This provides the unique opportunity to view not only information about the files moved but the actual files themselves, as described below.

If SafeGuard PortProtector is defined to work with Role-based permissions, then only administrators for whom the **View Shadow Files** Role Permission has been defined, can view shadowed files (See *Role Based (Advanced)*

To view the shadowed files:

1 Click the **Logs** tab.

2 Click the **File Logs** tab. Shadowed files have a checkmark in the **Shadow File** column and a sequential unique ID in the **Shadow File ID** column (See *The Log Table*).

3 Select the relevant Organizational Units (See *Filtering the Log Table by Organizational Unit*).

4 Define a new File Log query (See *Defining a New File Log Query*). Make sure to fill out the options in the **Shadowing** tab (See *Shadowing Properties – File Logs*).

5 Click **Run** to run the query.

6 Open the appropriate Logs Log Record Properties window.

7 Select **Open** or **Save** in the Shadow File column to download the shadowed file from the repository.

5.11 Reading Logs from a Standalone SafeGuard PortProtector Client Machine

You have the capability of reading logs from a standalone SafeGuard PortProtector Client machine. When applying the security policy on the standalone machine, configure the Client to store logs locally rather than send it to the Management Server over the network. This will prevent the agent from periodically attempting to send logs to the unavailable Management Server.

To configure a policy for storing logs locally:

1 In the *Policy* tab, under Settings (left pane) choose **Logging**.

2 In *Log Repository*, choose Set policy specific settings and select Store logs locally.

To read logs from a standalone Client:

3 On the Client machine, run the following command, which will ensure the logs currently used by the SafeGuard PortProtector Client are released, and can be copied off the machine:

sc control SophosSGPPS 222

4 Use the following command to copy the log files (*.slg) from their default location (%programfiles%\Sophos\SafeGuard PortProtector client\logs):

xcopy "[path to log files]" "[path to log file destination]" /c /i /Y

5 Transfer the log files from the standalone Client machine using a mass storage device or any other file transfer method.

Note: This process can easily be automated. Contact Sophos Support for obtaining a tool for transfering logs from standalone endpoints.

To import the logs to the Management Server:

1 Copy the logs to a machine running the SafeGuard PortProtector Management Console.

2 In the *Logs tab*, Choose **File>Manual log import**. The *Import Log* Files dialog box is displayed.

3 Choose Import logs from folder. Click Import.

4 In *Browse For Folder*, choose the folder containing the logs and click **OK**.

The logs will now appear in the Logs tab.

6 Managing Clients

About This Chapter

This chapter describes the Clients world, which serves as the central location for performing operations on the SafeGuard PortProtector Clients in the organization. The chapter includes the following sections:

- ***Overview*** provides a short description of the Clients World.
- ***Quick Tour of the Clients World*** described the main window in the Clients World.
- ***Clients Table*** describes the information available in the Clients Table and how to manage the table.
- ***Client Properties Pane*** describes the information and links in the Client Properties pane.
- ***Filtering Clients*** describes the tree and how you use it to display required Clients.
- ***Exporting the Clients Table*** describes how to export the Clients Table as an XML file which can be used by MS Excel for analysis purposes.
- ***Preparing to Deploy Clients*** provides information about what needs to be done prior to deploying SafeGuard PortProtector Clients to endpoints.
- ***Updating a Policy on a Client*** describes how to update a policy on a Client.
- ***Retrieving Latest Information from a Client*** describes how to collect logs in order to view the latest available information from Clients.
- ***Tracking Client Task Progress*** describes how to track the progress of Client tasks such as updating a policy or collecting logs.
- ***Temporary Suspension of Safeguard PortProtector Protection*** describes how to generate a password that enables temporary suspension of a Client.
- ***Resetting and Updating Client Status*** describes how to remove Clients that are Not Served from the Clients table.
- ***Deleting Clients that are not in Domain*** describes how to delete Clients that are Not in Domain.
- ***Auditing Devices*** describes how to launch SafeGuard PortAuditor from the Management Console.

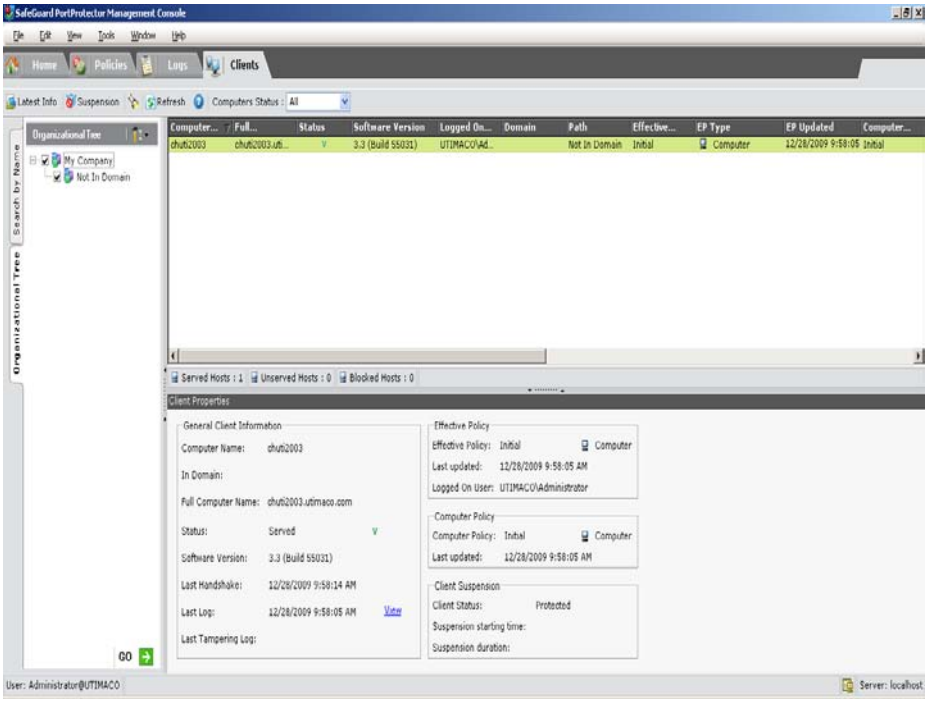
6.1 Overview

The Clients World serves as the central location for viewing the status and details of SafeGuard PortProtector Clients, performing tasks such as updating policies on Clients and collecting logs from Clients, viewing task progress, generating a password in order to temporarily suspend protection on a SafeGuard PortProtector Client and more.

6.2 Quick Tour of the Clients World

To access the Clients world:

Click the **Clients** tab. The Clients window appears:



6.2.1 File Menu

The *File* menu in the Clients World enables you to open other World windows, to export the Clients Table, to log out of the Management Console and to exit the application.

The *File* menu includes the following options:

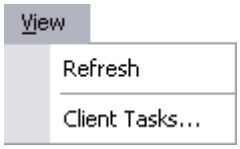
Option	Description
New	Opens a submenu that enables you to open a new policy window, a new Clients Log window, a new Server Log window or a new File Log window or a new report.
Change User Role	A SafeGuard PortProtector administrator can be assigned more than one role in order to define the various domain partitions for which they are responsible. After such an administrator logs in, a selection window is automatically displayed for selecting the role in which to work. **Note:** A User Role defines the functions, OUs and domains of an organization to which a SafeGuard PortProtector administrator has access, as described in *Defining Roles*. The **Change User Role** option enables such an administrator to change this role at any time to another role that has been assigned to him or her.
Export	Exports the Clients table to an external file.
Logout	Logs the current user out of the Management Console.
Exit	Logs out the current user and closes SafeGuard PortProtector Management Console.

6.2.2 Edit Menu

In the Clients world, the items in this menu are disabled.

6.2.3 View Menu

The *View* menu enables you to refresh the current window and to view the progress of Client tasks.



The *View* menu includes the following options:

Option	Description
Refresh	Updates the Clients table according to the Organizational Tree selection and refreshes Client table records according to current logs.
Client Tasks	Displays the progress of Client tasks (for details see *Tracking Client Task Progress*).

6.2.4 Tools Menu

The *Tools* menu which is common to all Worlds is described in *Tools Menu* in *Chapter 2: Getting Started*.

6.2.5 Window Menu

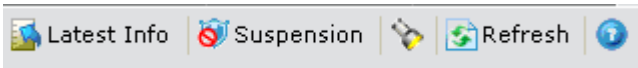
The *Window* menu which is common to all Worlds is described in *Window* Menu in Chapter 2: Getting Started.

6.2.6 Help Menu

The *Help* menu which is common to all Worlds is described in *Help* Menu in Chapter 2: Getting Started.

6.2.7 Toolbar

The Clients world toolbar provides quick access to some commonly used functions. It appears below the menu bar, and includes the following buttons:



The following is a brief description of each toolbar button:

Button	Description
Retrieve Latest Info	Click this button to get the most recent information from each Client by collecting logs (for details see *Retrieving Latest Information from a Client*).
Grant Suspension Password	Click this button to grant a suspension password in order to temporarily suspend protection from a Client.
Audit Devices	Click this button to launch SafeGuard PortAuditor (see *Auditing Devices*).
Refresh	Click this button t updates the Clients table according to the Organizational Tree selection and to refresh Clients table records according to current logs.
Help	Click to displays the context sensitive help of the active window and enables access to other help topics.

6.2.8 Workspace

The Clients world workspace is divided into three areas:

- **Clients Table** - appears in the top right pane and displays a table of the Clients in the selected Organizational Tree component. Before you make any selection in the **Organizational Tree** or **Search By Name** tabs (described below) this area is empty. Refer to *Clients Table* for more details.
- **Organizational Tree** and **Search By Name** tabs – appear on the left-hand side pane. These tabs serve as filters for determining which records are displayed in the Clients Table. The tabs are discussed in *Filtering Clients*.
- **Client Properties** pane - appears below the Client Table and displays the properties of the computer selected in the Clients table. Refer to *Client Properties Pane* for more details.

6.3 Clients Table

The Clients table displays information about the Clients protecting the organizational component(s) selected in the Organizational Tree.

The Clients table displays the following columns:

Column	Description
Computer Name	The name of the computer to which the columns in the row refer.
Full Computer Name	The full name of the computer to which the columns in the row refer, including its domain as a suffix.
Status	**Served** ( ) – protected by SafeGuard PortProtector Client or **Not Served** ( ) – not protected.
Software Version	The version of SafeGuard PortProtector installed on the computer.
Logged On User	If a user is logged on, displays user name and domain name.
Domain	Domain name.
Path	Path to Client location in Active Directory/Novell eDirectory.
Effective Policy (EP)	The name of the policy which is in effect on the computer. If policies are merged on this Client, all merged policies are listed.
EP Type	The effective policy type - **computer** ( ) or **user** ( ).
EP Updated	The date and time the effective policy was last updated.

Column	Description
Computer Policy (CP)	The name of the computer policy. This may be different than the Effective Policy if a user policy is in effect.
CP Updated	Date and time the computer policy was last updated.
Last Handshake	The date and time of the last handshake between the Client and the Management Server.
Received Logs	The date and time logs were last received.
Received Tampering Logs	The date and time tampering logs were last received.
Suspension Status	**Suspended** - protection is suspended, otherwise **Protected**.
Suspension Start Time	The date and time that suspension began.
Suspension Duration	The period defined by the administrator for which this computer will be suspended.

You can modify the table view in the following ways:

- **Sort** the table by clicking the column heading of the column by which you wish to sort. Clicking the header again switch from ascending to descending order. You can and a secondary sort level by pressing the **Shift** key and clicking the secondary column heading.
- **Modify column width** by dragging the column separation lines.
- **Move a column** by dragging and dropping it into the desired position.

6.4 Client Properties Pane

The *Client Properties* pane appears below the Clients table, and displays the properties of the Client you select in the table. The details in this pane are identical to the details displayed in the table. The pane displays information regarding the selected table record, arranged in the following sections:

- **General Client Information:** displays general information about the computer and the Client. Includes an indication as to whether the Client is Served or not, a link for viewing logs for the Client and a link for viewing tampering logs for the Client. A hazard icon is displayed if this computer has been tampered with at least once.
- **Effective policy:** displays information about the currently effective policy (the effective policy is different from the Computer Policy when a user who has a User Policy is logged on). Includes a link for viewing the effective policy.
- **Computer policy:** displays information about the Computer Policy (the Computer Policy may not be the currently effective policy if a user who has a User Policy is logged on). Includes a link for viewing the Computer Policy.
- **Client Suspension information**: displays information concerning Client suspension. A hazard icon is displayed if this computer is currently suspended.

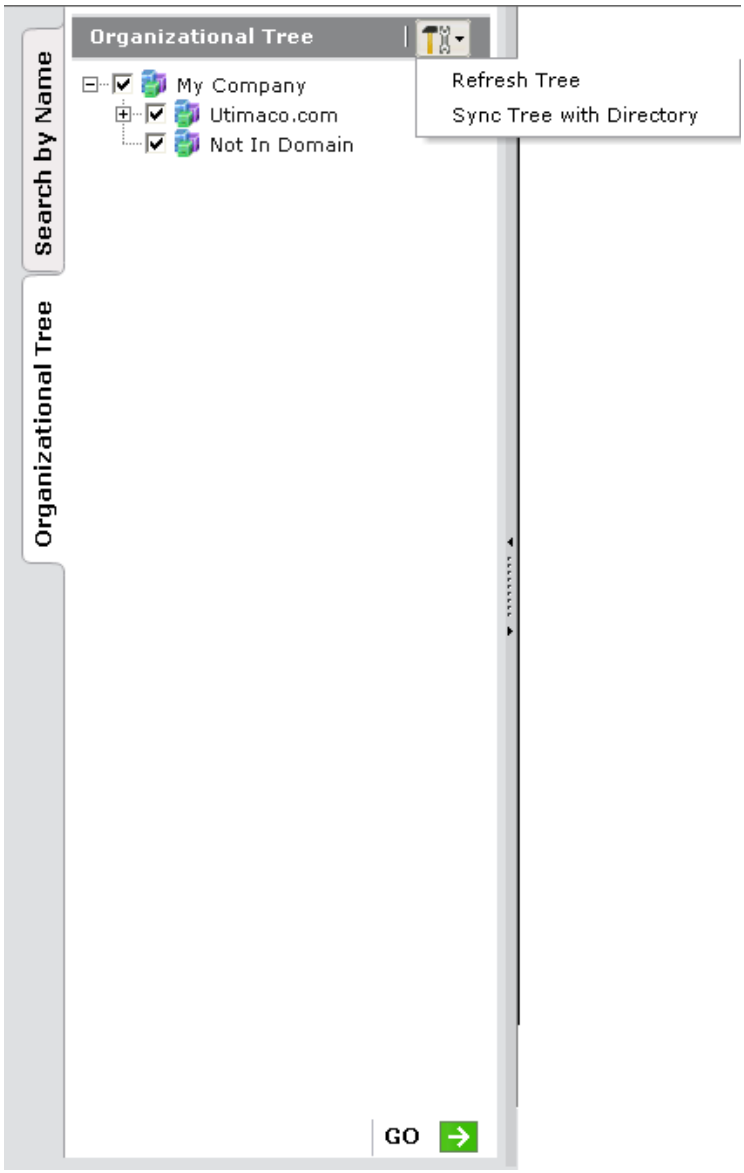
6.5 Filtering Clients

The left-hand side of the Clients window includes two tabs to help you determine the computers whose information will be displayed in the Clients Table.

6.5.1 Filtering the Clients Table by Organizational Unit

The *Organizational Tree* is a tool you use to determine the Organizational Units from which Clients will be displayed in the Clients Table. This section describes how to manage the Organizational Tree and how to determine, from the Tree, which Clients are displayed in the Clients Table.

The *Organizational Tree* tab displays the domain(s), organizational units and the Not In Domain group (which includes all computers who do not currently belong to the domain), as shown in the following figure:



Note: The Organizational Tree is applicable only if you are using Active Directory/Novell eDirectory. If you are not, only one group is displayed in the Tree – Not In Domain. Selecting this group selects all computers.

To select the required organizational units:

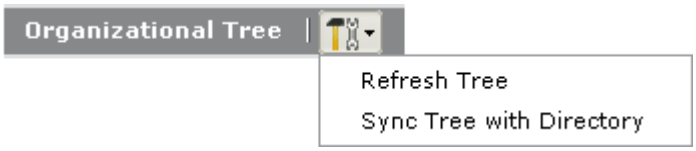
1 If necessary, expand the Organizational Tree to view lower-level organizational units.

2 Select the required domain or organizational units by checking the appropriate checkboxes.

3 At the bottom of the *Organizational Tree* tab, click **GO** ( ). The information now displayed in the Clients Table originates from Clients that belong to your Tree selection, and only them.

6.5.1.1 Updating the Organizational Tree

Before you make your selection in the Tree, you may want to update it. You can either refresh the Tree from SafeGuard PortProtector Management Server, or synchronize it with Active Directory/Novell eDirectory (the Directory may be more up-to-date, but may also take longer). Updating the Tree is done from the *Organizational Tree Update* menu (shown below) which is found at the top of the Organizational Tree tab.



To update the Organizational Tree from the Management Server:

From the *Organizational Tree Update* menu, click **Refresh Tree**. The Tree is updated.

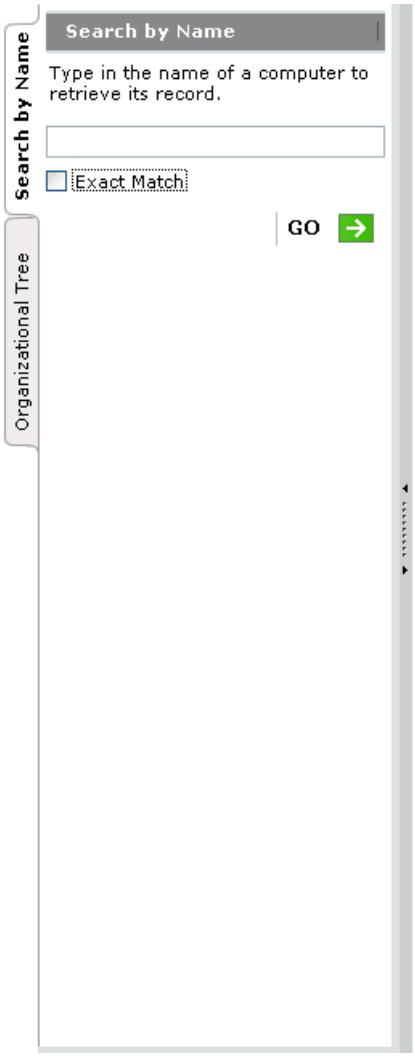
To update the Organizational Tree from the Directory:

From the *Organizational Tree Update* menu (see previous figure), click **Sync Tree with Directory**. The Tree is updated, but this may take a while.

6.5.2 Filtering by Name

The *Search by Name* tab is an additional tool that you can use to determine the computers whose records the Clients Table will display. This section describes how to use this tab to determine the Clients displayed in the Clients Table.

The following figure shows the *Search by Name* tab:



To search for specific computers:

1 In the text box, enter the name of the computer whose record you wish to display in the table. You may enter multiple names separated by comma, semicolon or space.

2 Check the **Exact Match** checkbox if you want the table to display records for a computer with the name that exactly matches the string you entered in the text box. In this case you must enter the full computer name (including the domain suffix). If **Exact Match** is not selected, the Clients Table will contain records for all computers whose name contains the string that you entered.

3 Below the text box, click **GO** ( ). The Client records now displayed in the table refer the computer/s whose name matches your search criteria. If no computer is found whose name matches your search criteria the table is empty.

6.6 Exporting the Clients Table

If you want to export the Clients Table to an external file in order to print it or perform further analysis you can do so from the *Export Clients* window.

To open the *Export Clients* window:

From the *File* menu, select **Export**. The *Export Clients* window opens.

6.6.1 Exporting the Clients Table to an External File

Use this option to export the Clients Table in order to print it or perform further analysis you can do so. The exported file is saved in XML format which can easily be opened with MS Excel etc.

To export Clients:

1 Click **Browse** to select a path (and type a file name) or type in the path for the exported file.

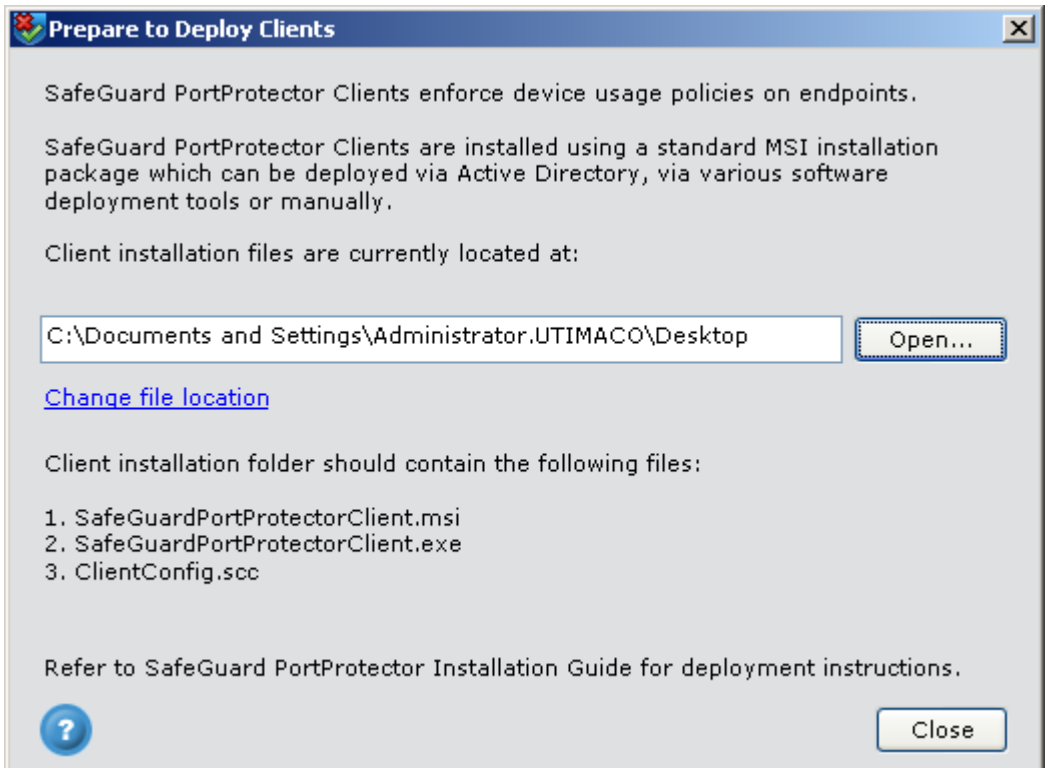
2 Click **OK**. A progress window opens and exporting begins.

6.7 Preparing to Deploy Clients

SafeGuard PortProtector Client deployment (installation) is performed with a standard MSI installation package. The installation can be performed via Active Directory, various other deployment tools or manually. Before performing deployment, you can check to verify that the required files are available.

To prepare for Client installation:

From the *Tools* menu, click **Prepare to Deploy Clients**. The *Prepare to Deploy Clients* window opens:


Prepare to Deploy Clients
SafeGuard PortProtector Clients enforce device usage policies on endpoints.
SafeGuard PortProtector Clients are installed using a standard MSI installation package which can be deployed via Active Directory, via various software deployment tools or manually.
Client installation files are currently located at:
C:\Documents and Settings\Administrator.UTIMACO\Desktop
Open...
Change file location
Client installation folder should contain the following files:
1. SafeGuardPortProtectorClient.msi
2. SafeGuardPortProtectorClient.exe
3. ClientConfig.scc
Refer to SafeGuard PortProtector Installation Guide for deployment instructions.
Close

6.7.1 Prepare to Deploy Clients

This window displays the current location of the SafeGuard PortProtector Client installation files. The location of the Client installation files is defined in the Clients tab in Administration (refer to Chapter 7, Administration).

The Client installation folder should contain the following files:

- SafeGuardPortProtectorClient.msi
- SafeGuardPortProtectorClient.exe
- ClientConfig.scc

For a detailed explanation of Client installation please refer to *SafeGuard PortProtector Installation Guide*.

To prepare for Client deployment:

In the window, click **Open** and check that the required files are in the installation folder. If they are not, you can go to the *Administration* window by clicking the Change file location link.

Complete instructions for deploying SafeGuard PortProtector Clients can be found in *SafeGuard PortProtector Installation Guide*.

6.8 Updating a Policy on a Client

Note: Since SafeGuard PortProtector uses WMI for this option, if you selected Novell as your Directory in the *Administration* window you will be able to perform this action only if a Windows user with local administrative rights is defined on the target endpoint(s).

As explained in *Chapter 4, Distributing Policies*, policies are updated on SafeGuard PortProtector Client by means of the Client checking the GPO service or the registry file at predefined intervals, and updating the policy if it has changed. If you have recently edited a policy for a certain Organizational Unit or computer, you may wish to notify the relevant SafeGuard PortProtector Clients to check for an updated policy at the earliest possible opportunity.

There are two options for updating policies:

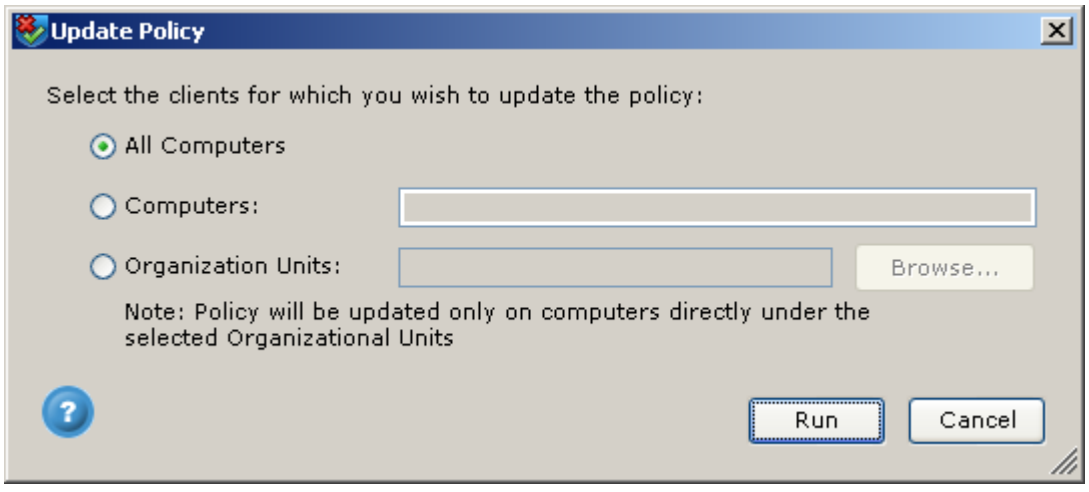
- **From the Tools menu**: this option enables you to update policies by any Organizational Unit or computer.
- Using **right-click:** this option enables you to update policies on pre-selected Clients by right-clicking Organizational Units from the Organizational Tree, or by right-clicking served Clients in the Clients table.

6.8.1 Updating a Policy on Any Client

Updating a policy is activated from the *Update Policy* window.

To open the *Update Policy* window:

In the *Tools* menu, select **Update Policy**. The *Update Policy* window opens:



6.8.1.1 Updating a Client Policy

If you have recently edited a policy for a certain Organizational Unit or computer, you may wish to notify the relevant SafeGuard PortProtector Clients to check for an updated policy at the earliest possible opportunity.

To update a policy:

1 Select the required radio button option, as follows:

- **All Computers**: Click this option if you wish to update policies on all the computers in the organization.
- **Organizational Unit**: Click this option if you wish to update policies one or more organizational units, click **Browse**, and select the desired organizational units from the company tree. The selected units appear in the **Organizational Unit** field.
- **Computer**: Click this option if you wish to update a policy for one or more computers and type the computer name in the field. To type more than one computer name, use a colon or a semi-colon as a delimiter.

2 Click **Run**. Notification is sent to the selected computers to check for a new policy, and the *Client Task Progress* window opens. You can track the progress of the update process in this window as explained in *Tracking Client Task Progress*.

6.8.2 Updating a Policy on Pre-selected Clients

This option performs the same action described in the previous section, but allows you to pre-select the Clients on which to perform the update.

To update policies (using right-click):

1 In the Company Tree, select the desired components, OR select the desired computers in the table.

2 Right–click. In the menu that appears, select **Update Policy**. Notification is sent to the selected computers to check for a new policy, and the *Client Task Progress* window opens. You can track the progress of the update process in this window as explained in *Tracking Client Task Progress*.

6.9 Retrieving Latest Information from a Client

Note: Since SafeGuard PortProtector uses WMI for this option, if you selected Novell as your Directory in the *Administration* window you will be able to perform this action only if a Windows user with local administrative rights is defined on the target endpoint(s).

You may at times wish to view Client information as close to real time as possible. This option enables you to collect logs and view the latest information from served computers outside the predefined collection times. Activating this function collects all log types.

There are two ways to collect logs:

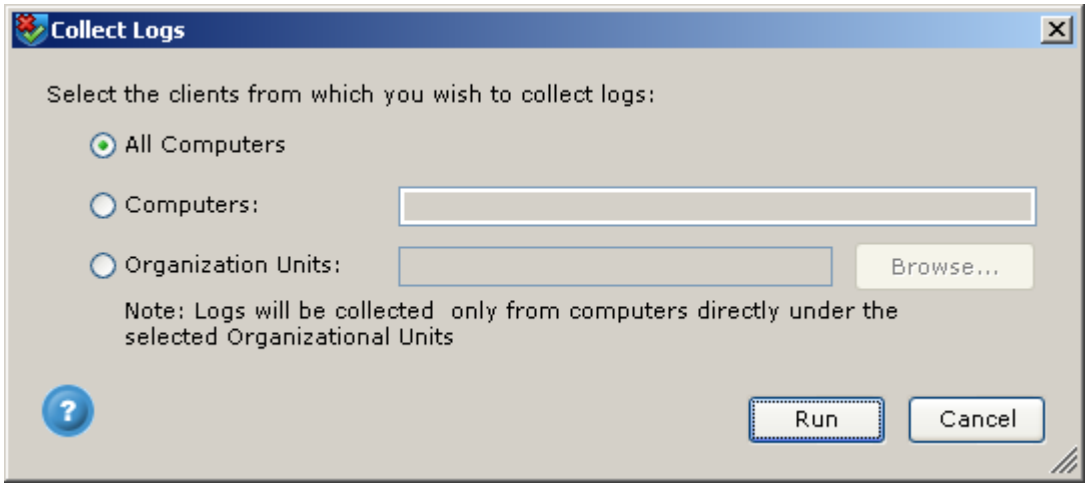
- **From the *Tools* menu or the toolbar**: this option allows you to collect logs by any organizational unit or computer.
- **Using right-click:** this option enables you to collect logs from pre-selected Clients by right-clicking Organizational Units from the Organizational Tree, or by right-clicking served Clients in the Clients table.

6.9.1 Collecting Logs from Any Client

Log collection is activated from the *Collect Logs* window.

To open the *Collect Logs* window:

In the *Tools* menu, select **Retrieve Latest Info** (**collect logs**), or click the **Retrieve Latest Info button** in the toolbar. The *Collect Logs* window appears:



6.9.1.1 Collecting Logs

This option enables you to collect logs and view the latest information from served computers outside the predefined collection times. Activating this function collects all log types.

To collect logs:

1 Click the radio button for the desired option, as follows:

- **All Computers**: Mark this option if you wish to collect logs from all the computers in the organization.
- **Organizational Unit**: Mark this option if you wish to collect logs from one or more organizational units, click **Browse** and select the desired organizational units from the company tree. The selected units appear in the **Organizational Unit** field.
- **Computer**: Click this option if you wish to collect logs from one or more computers and type the computer name in the field. To type more than one computer name, use a colon or a semi-colon as a delimiter.

2 Click **Collect Now**. Log collection from the selected computers begins, and the *Client Task Progress* window opens. You can track the progress of the update process in this window as explained in *Tracking Client Task Progress*.

6.9.2 Collecting Logs from Pre-selected Clients

This option performs the same action described in the previous section, but allows you to pre-select the Clients from which to collect logs.

To collect logs (using right-click):

1 In the Company Tree, select the desired nodes.

2 Right-click. A menu opens.

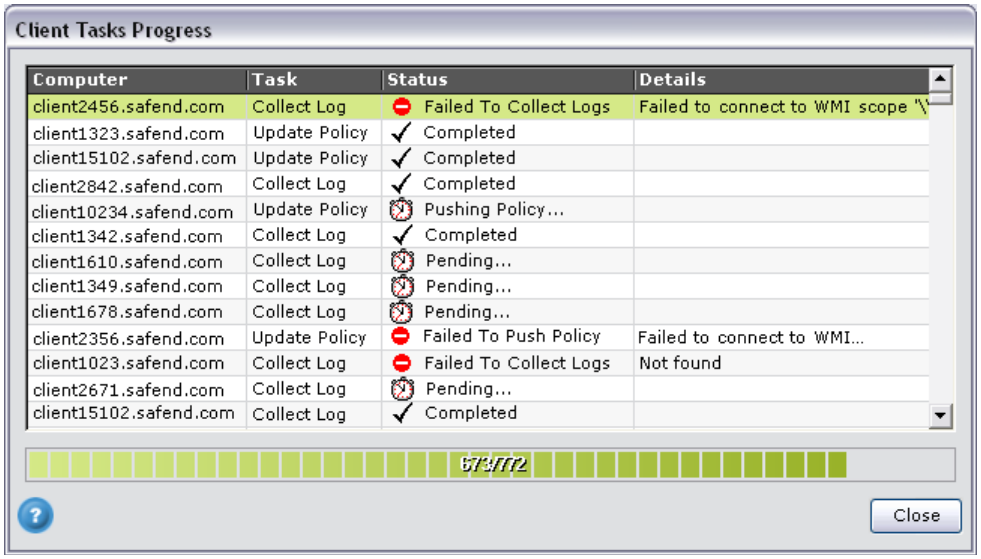
3 In the menu, select Retrieve Latest Info. Log collection from the selected computers begins, and the *Client Task Progress* window opens. You can track the progress of the update process in this window as explained in *Tracking Client Task Progress.*

6.10 Tracking Client Task Progress

When the application is in the process of performing tasks (such as collecting logs or updating policies), you may view the progress of these tasks in the *Client Tasks Progress* window.

To track Client task progress:

From the *View* menu, select **Client Tasks**. The *Client Tasks Progress* window opens. You can view task progress in this window.



6.10.1 Client Task Progress

The *Client Task Progress* window displays all the tasks running at that moment, with the status of each task, and changes in this status as they occur. It displays a single line for each Client (unless a policy updating task and a log collection task for the same Client are running concurrently, in which case two lines are displayed for this Client). As the phases in the task change, so does the value in the *Status* column. A finished task has a status of **Completed** or **Failed**. In the case of a failed status, a reason is supplied.

The *Client Tasks Progress* window menu includes the following columns:

Option	Description
Computer	Displays the full computer name.
Task	Displays the task which the Client is performing (Collect log, Update Policy).
Status	Displays the current task status (Completed, Pending, Pushing Policy, Failed).
Details	When Status is Failed, displays the reason.

Note:

Since SafeGuard PortProtector uses WMI for performing remote client tasks, WMI ports must be open for the command to go through. See *Client Tasks Failure* for additional information.

Note:

If you selected Novell as your Directory in the Administration window you will be able to perform this action only if a Windows user with local administrative rights is defined on the target endpoint(s).

6.10.1.1 Client Tasks Failure

Since SafeGuard PortProtector uses Windows WMI infrastructure for performing remote client tasks, WMI ports must be open for the command to go through. There may be 3 different types of cases where the WMI command will not function correctly. If one or more Client Tasks have failed, check the following according to the task details displayed in the **Details** column of the *Client Tasks Progress* window:

Task Details	Resolution
Access Denied	Make sure the defined Server Credentials, used for performing the scan, include local administrator privileges on the remote machine. You may refer to *Server Credentials* for more information.
The service cannot be started	Make sure the WMI service on the remote machine is started and set to start automatically.
The RPC server is unavailable	Make sure WMI ports are allowed on the active firewall, and that "remote administration" is allowed in the Windows Firewall.

To Verify WMI connectivity on your environment:

1 From the Server machine, Select **Run** from the *Start* menu, type wmimgmt.msc.

2 On the left hand side, right click **WMI Control** (**Local**) and select **connect to another computer**.

3 Select another **computer** and enter the name of the computer with which you are trying to establish communication. Click **OK**.

4 On the left hand side, right click **WMI Control** [**hostname**] and Select **Properties**. The application scans the remote machine using WMI.

5 The scan result indicates the status of the WMI connectivity between the SafeGuard PortProtector Management Server and the target machine.

6.11 Temporary Suspension of SafeGuard Protection

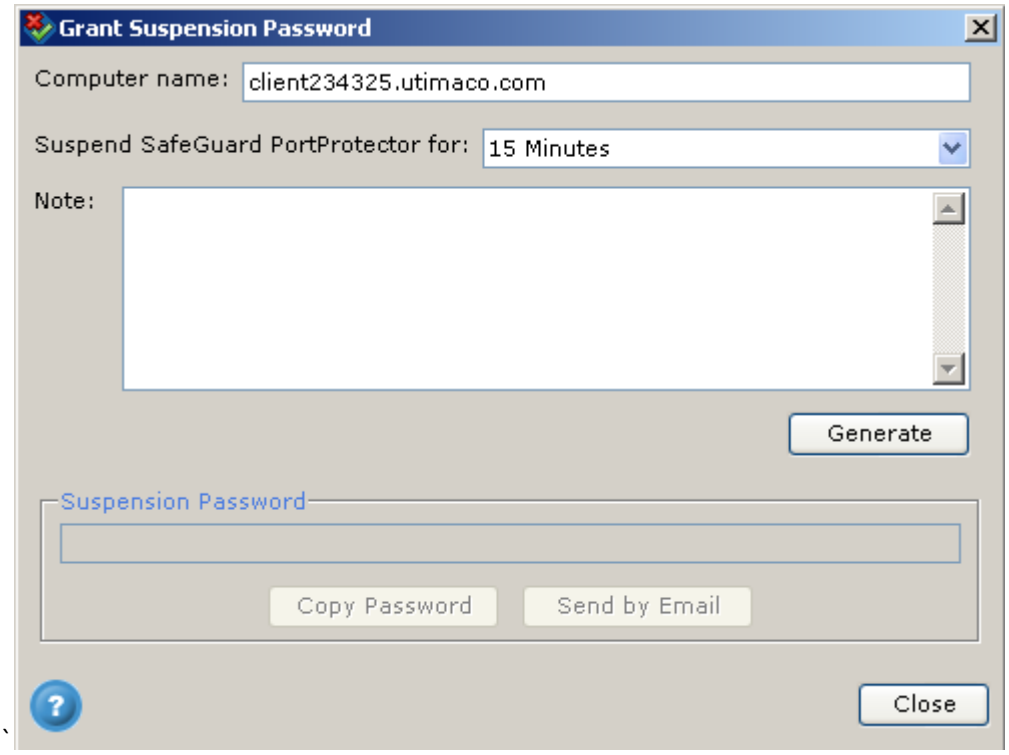
At times it may be necessary to temporarily suspend SafeGuard Protection on a Client without uninstalling the SafeGuard PortProtector Client. An example might be a user who is away from the office, with a laptop that needs to have an unauthorized disk-on-key connected to it on a one-time basis in order to view an important presentation which resides on that disk-on-key.

The end-user requires a password in order to perform suspension. This password is generated by the administrator and is provided to the user. Suspension begins once the user enters the password, and is pre-set for a limited period of time. Once this period ends, protection of the Client is resumed.

Once protection is resumed, Client logs are updated with information about the suspension, about devices which were connected during the suspension period and about files copied to and from those devices.

To open the Grant Suspension Password window:

In the Clients table, right-click the computer on which you wish to suspend protection, and select **Grant Suspension Password**. Alternatively, you can click the **Grant Suspension Password** button in the tool bar, or select this option from the *Tools* menu. The following window opens:



6.11.1 Granting a Suspension Password

Use the *Grant Suspension Password* window to enter the necessary information about the computer on which protection is to be suspended, to enter suspension parameters and to generate a suspension password which you will provide to the user.

To grant a suspension password:

1 If the **Computer Name** field is empty (which may be the case when you open this dialog from the *Tools* menu or using the toolbar button), enter the required computer name.

2 In the **Suspend SafeGuard Protection for** field, select the suspension period from the drop-down menu.

3 In the **Notes** field, enter any text you desire, for example a description of the reason for suspension (optional).

4 Click **Generate**. The system generates a password and displays it.

5 Click **Copy Password** to copy the password to the clipboard, or **Send by Email** to open a new message in your email application containing all suspension information (computer name, suspend period, notes and password).

6.12 Resetting and Updating Client Status

With time, Clients that were previously Served may not always remain Served. This option allows you to reset the status of SafeGuard PortProtector Clients which appear as Served in the Clients table but may currently be Not Served.

To reset and update a Client's status:

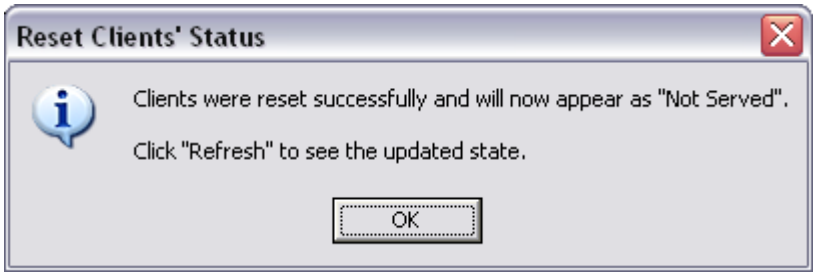
In the Clients table, right-click the Served Client which you wish to reset.

OR

1 In the Organizational tree, right click the desired object.

2 A menu opens.

3 From the menu, select **Reset Client Status**. The following window opens:


Reset Clients' Status
Clients were reset successfully and will now appear as "Not Served".
Click "Refresh" to see the updated state.
OK

Note:

The **Reset Client Status** option is enabled only for Served Clients.

Note:

In the Clients Table, you may select multiple Clients to reset. In the Organizational Tree, selecting an object (e.g. an OU or a domain) will reset all Clients belonging to this object.

4 From the toolbar, click **Refresh**. Client status is updated and Not Served Clients that previously appeared as Served now appear with their correct status, Not Served.

Note:

Clients that were reset will show as Served again once they communicate with the server.

6.13 Deleting Clients that are not in Domain

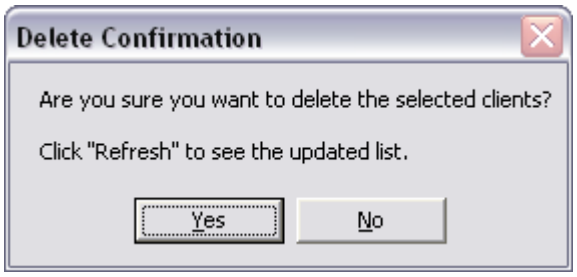
As explained earlier, the Organizational Tree may include Clients that no longer belong or never belonged to any of the tree domains and are represented in the tree under Not in Domain. Some of these Clients may no longer relevant and you may wish to delete them from the Tree. You may choose either to delete all Not in Domain Clients (both Served and Not Served), or to delete specific Clients that are Not in Domain.

Note: A Client is added as Not in Domain as soon as it communicates with the server and is found not to belong to any Tree domain.

To delete all Not in Domain Clients:

1 In the Organizational Tree, right-click Not in Domain. A menu opens.

2 From the menu, select Delete Clients. The following confirmation window opens:



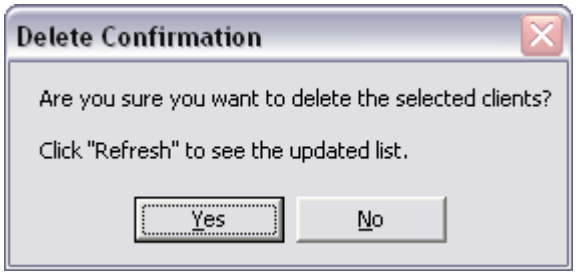
3 Click **Yes**. All Clients that are Not in Domain are deleted.

4 From the toolbar, click **Refresh**. The deleted Clients are no longer displayed.

To delete specific Clients that are Not in Domain:

5 In the Clients table, right-click the required Client (you may delete a Client that is Not in Domain regardless of whether it is Served or Not Served). A menu opens.

6 From the menu, select Delete Clients (Not in Domain). The following confirmation window opens:



7 Click **Yes**. All selected Clients that are Not in Domain are deleted.

8 From the toolbar, click **Refresh**. The deleted Clients are no longer displayed.

6.14 Auditing Devices

If you wish to check which devices are currently, or were previously, connected to your organization's endpoints, you may audit them. Auditing devices is done using SafeGuard PortAuditor, our scanning and auditing tool described in detail in *SafeGuard PortAuditor User Guide*. If you wish, you may launch SafeGuard PortAuditor directly from SafeGuard PortProtector.

To launch SafeGuard PortAuditor:

Click the **Audit Devices** tool button. The first time you do this, you will be asked to browse to the location of your auditor.exe file. Subsequently, after you have done this once, SafeGuard PortAuditor is launched and its main window opens.

7 Administration

About This Chapter

This chapter describes the *Administration* window, its parameters and the administrative considerations when setting up SafeGuard PortProtector.

This chapter contains the following sections:

- ***Administering SafeGuard PortProtector*** describes the situations when you may need to administer SafeGuard PortProtector and how to open the *Administration* window in which you can do so.
- ***Administration Window*** describes the various settings in the seven tabs provided in the *Administration Settings* window.

7.1 Administering SafeGuard PortProtector

When SafeGuard PortProtector is first launched following installation, the system is initialized with default settings that may be applicable to the majority of users.

During the ongoing operation of SafeGuard PortProtector, you may want to update various administration settings. This is performed in the *Administration* window, as follows.

To open the Administration window:

From the *Tools* menu, select **Administration**

OR

In the Home World, from the *More* section, click the **Change Administration Settings** link.

The *Administration* window opens.

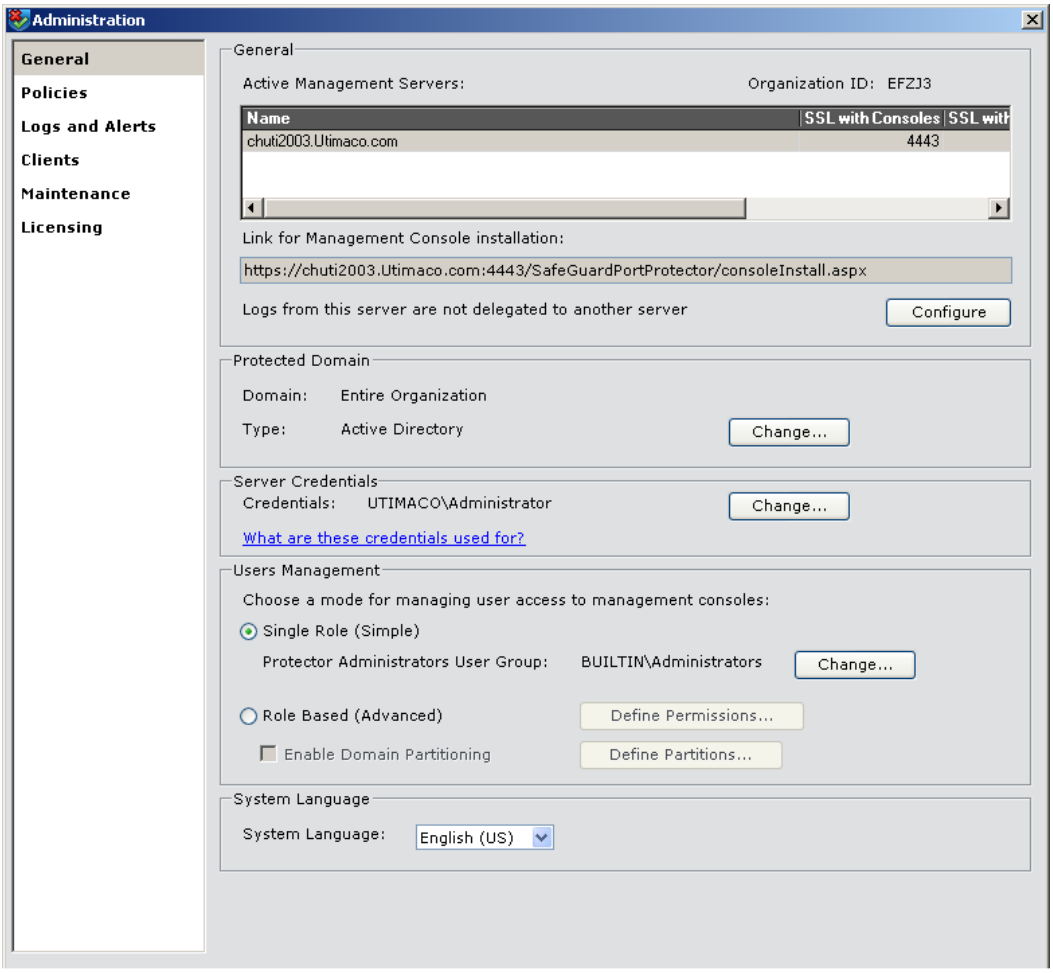
7.2 Administration Window

The settings in the *Administration* window consist of six tabs:

- **General**, described in *General Tab Settings*.
- **Policies**, described in Configuring General Tab Settings
- **Logs and Alerts**, described in *Configuring Logs and Alerts Tab Settings.*
- **Clients**, described in Configuring Clients Tab Settings
- **Maintenance**, described in *Configuring Maintenance Tab Settings*.
- **Licensing** tab, as described in Configuring Licensing Tab Settings.

7.3 General Tab Settings

General administration settings are defined in the *General* tab of the *Administration* window:



7.3.1 Configuring General Tab Settings

The *General* tab enables you to configure general system configuration parameters for SafeGuard PortProtector. It contains the following sections:

- Protected Domain
- *Server Credentials*
- *Users Management*

Note: Whenever you modify any of the settings in this tab you must click **OK** at the bottom of the *Administration* window for the modifications to apply.

7.3.1.1 General

These fields contain information about the Management Server in which SafeGuard PortProtector is managed. Each SafeGuard PortProtector Server is a computer on which you have installed the SafeGuard PortProtector Console and the SafeGuard PortProtector Management Server applications. Each SafeGuard PortProtector Console works with the SafeGuard PortProtector Management Server on which it was installed. The Management Server has multiple roles:

- It is used as a central point for communicating with SafeGuard PortProtector Clients installed on endpoints.
- It holds a database of all system configuration, policies and logs.
- It communicates with Management Consoles.

Following are the properties in this section:

- **Active Management Servers** – This grid lists the SafeGuard PortProtector Management Servers that are active.
- **Server Name** – This field shows the full name of the computer on which the SafeGuard PortProtector Server is running. Next to it, in parentheses, appears a string representing the unique encryption key which was generated during installation (for example P8G2U). This string is used to verify that the Clients hold the same encryption key and to debug encryption key issues. These fields are not configurable.
- **Server port** – This field shows the TCP ports on which the Management Server performs its communications with the Clients (controlling and collecting log) and with the management consoles (defining policies, reviewing logs, etc.).

All Management Server communications performed over these TCP ports are encrypted using SSL.

During installation on Windows 2003, port 4443 is used as a default for Server-Console SSL communications and port 443 is used as a default for Server-Client SSL communications. During installation on Windows XP, port 443 is used as the default port for both Server and Client SSL communications. If for any reason you wish to change the port number, you can change it from the Microsoft IIS settings on the Management Server machine.

To change the port, follow the steps below:

1 Access the IIS settings from the control panel of your Management Server machine (administrative tasks → Internet Information Services).

2 Locate the SafeGuard PortProtector site:

- On Windows XP this is "Default Web Site"
- On Windows 2003 locate two web sites: "SafeGuard PortProtector Web Site" for Management Console communications (default port 4443) and "SafeGuard PortProtector Web Site WS" for Client communications (default port 443)

3 Change the SSL port(s) to your desired port(s).

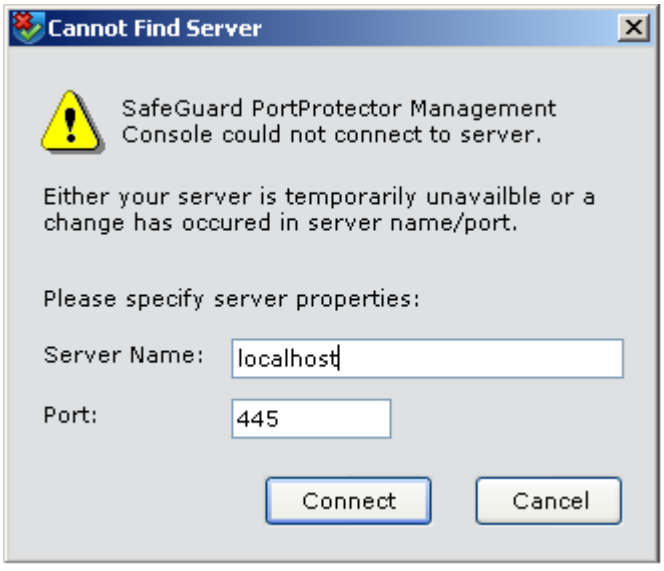
4 Kill the IIS worker process on your Management Server:

- On Windows XP this is "aspnet_wp.exe"
- On Windows 2003 this is "w3wp.exe"

5 Access the SafeGuard PortProtector Management Console from the local machine and perform any kind of change in the "Global Policy Settings" in order to cause re-publish of all policies.

Note:

- Since all Clients and Management Consoles use this port for communicating with the Management Server, changing the port will cause them to cease from communicating with the Server until they are notified of the new port.
- Never change the port during active hours. If multiple management consoles are now in use, changing the port will cause immediate disconnection of these consoles, resulting in possible data loss.
- SafeGuard PortProtector Clients communicate with the Management Server in the communication port specified in their policy. Once you change the port, Clients will not be able to communicate with the Management Server until they receive the re-published policies.
- Management Console administrators need to be notified of the port change. You may choose one of the following options:
- Require administrators to re-install the Management Console by using the Management Console Installation web page. You will need to notify them of the new address (see following this note).
- Communicate the new port to your administrators. They will need to manually insert it the next time they open the Management Console, in the following window:



- **Link for management console installation:** Typically, Management Consoles are deployed via a web page on the Management Server machines which allows users to download the Management Console installation package and install it on their machine.
- The link is in the following format:

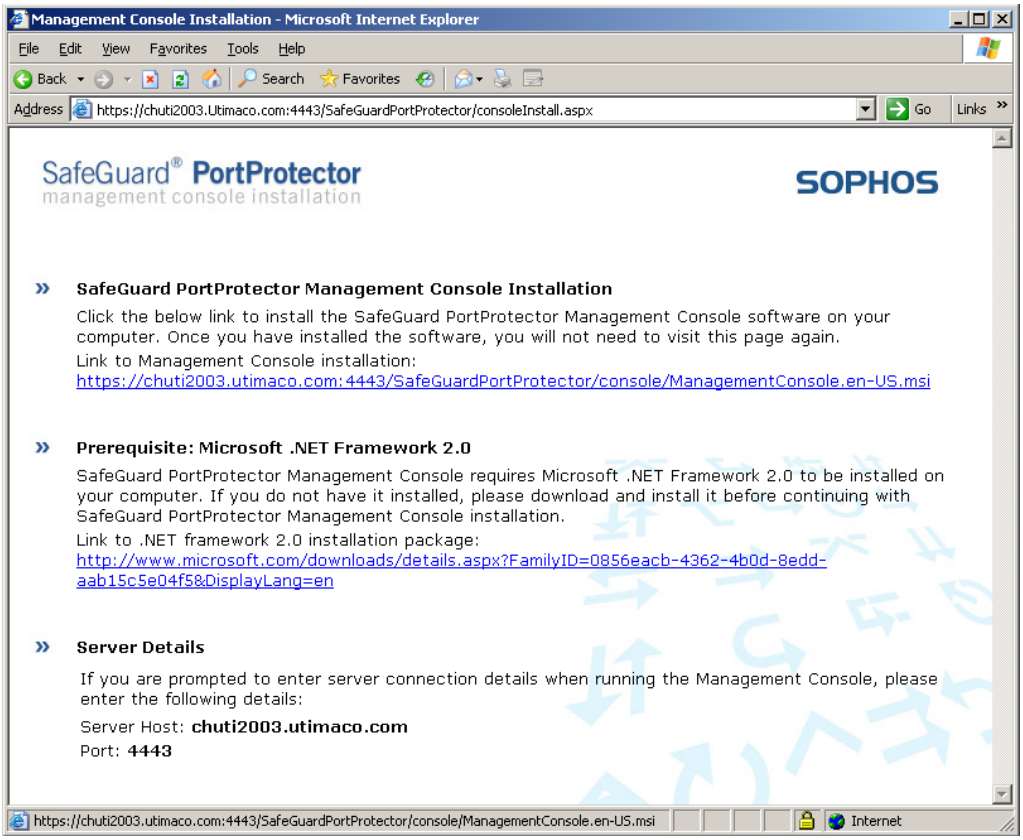
```
https://<servername>:<serverport>/
SafeGuardPortProtector/consoleinstall.aspx
```

Tip:

You may also use a shorter link format:

```
https://<servername>:<serverport>/
SafeGuardPortProtector
```

In order to install the Management Console on a new machine, all you need is to notify the user of this web page address. The following window opens:


Management Console Installation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://chuti2003.Utimaco.com:4443/SafeGuardPortProtector/consoleInstall.aspx
Go Links
SafeGuard® PortProtector
management console installation
SOPHOS
SafeGuard PortProtector Management Console Installation
Click the below link to install the SafeGuard PortProtector Management Console software on your computer. Once you have installed the software, you will not need to visit this page again.
Link to Management Console installation:
https://chuti2003.utimaco.com:4443/SafeGuardPortProtector/console/ManagementConsole.en-US.msi
Prerequisite: Microsoft .NET Framework 2.0
SafeGuard PortProtector Management Console requires Microsoft .NET Framework 2.0 to be installed on your computer. If you do not have it installed, please download and install it before continuing with SafeGuard PortProtector Management Console installation.
Link to .NET framework 2.0 installation package:
http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&DisplayLang=en
Server Details
If you are prompted to enter server connection details when running the Management Console, please enter the following details:
Server Host: chuti2003.utimaco.com
Port: 4443
https://chuti2003.utimaco.com:4443/SafeGuardPortProtector/console/ManagementConsole.en-US.msi
Internet

Note:

You may also choose to use the installation package itself to install the Management Console. This package is also available on your CD under the name ManagementConsole.msi

7.3.1.2 Log Delegation

Note: If you are planning to implement this feature, please consult with Sophos support first to verify that this is indeed the appropriate architecture for your environment.

This feature enables you to view in a single management server, logs from other management servers.

Important:

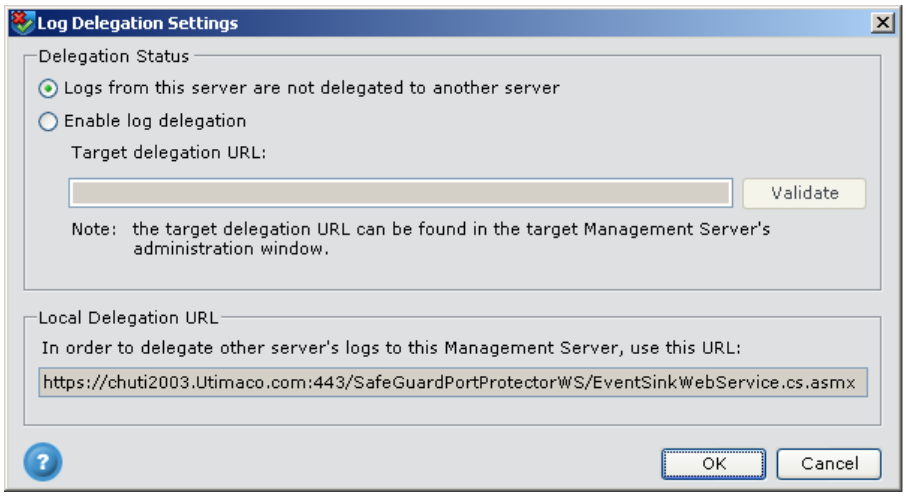
Here are some important points to note:

1. All the servers must be installed with the same encryption keys (using the *restore* option during server installation).
2. The Delegation Server should be used only to view logs from other servers, and not for applying policies or managing clients. It is recommended to choose role-based users management (see *Users Management*) and a user with log reviewer privledges only.
3. It is recommended that this option be used only where the environment has several domain fore*sts*.

To configure log delegation:

1 From the target server (Delegate server) in the Management Console, choose **Administration** from the Tools menu.

2 At the top of the General tab, click the **Configure** button beside, "Logs from this server are not delegated to another server". The *Log Delegation Settings* window is displayed.

3 
Log Delegation Settings
Delegation Status
Logs from this server are not delegated to another server
Enable log delegation
Target delegation URL:
Validate
Note: the target delegation URL can be found in the target Management Server's administration window.
Local Delegation URL
In order to delegate other server's logs to this Management Server, use this URL:
https://chuti2003.Utimaco.com:443/SafeGuardPortProtectorWS/EventSinkWebService.cs.asmx
OK
Cancel

4 Copy the URL in the *Local Delegation URL* and save it to a file so it can be used on the delegating servers installed on other machines.

5 In each of the servers whose logs will be read, in the Management Console enter the Log Delegation Settings window.

6 In *Delegation Status* select, **Enable log delegation**.

7 Copy the URL from the target server to the *Target delegation URL* field.

8 Click the **Validate** button to validate this URL. Click the **OK** button to save the settings.

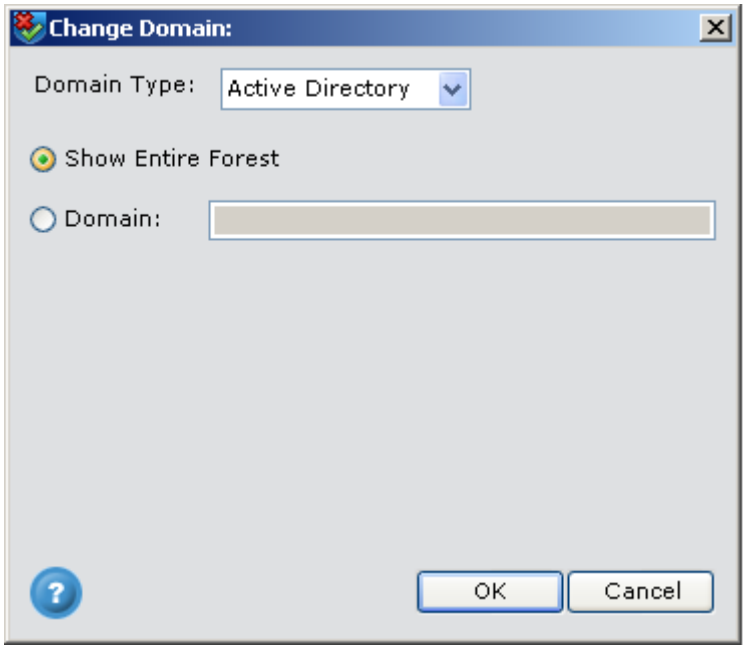
A copy of all client and file logs from these servers will now be sent to the target server.

7.3.1.3 Protected Domain

This section defines the protected domain and whether it is an Active Directory or a Novell eDirectory domain. These definitions are set in the *Change Domain* window.

To open the Change Domain window:

In the Protected Domain section, click **Change**. The *Change Domain* window opens:



Define the required settings as explained in *Defining Protected Domain* below.

7.3.1.3.1 Defining Protected Domain

This window is where you define the protected domain and its type.

To define domain type:

1 In the *Domain Type* menu, select **Active Directory** or **Novell eDirectory**, as required.

Note: If you are using Novell eDirectory please refer to *Appendix A – Novell eDirectory Synchronization*.

2 Click the appropriate radio button to select whether you want to display the **entire forest** or only a specific **domain**. If you want to display a specific domain, enter its name.

3 Click **OK** to save and exit.

7.3.1.4 Server Credentials

For the Management Server application to perform its functions on the network, a user account with sufficient privileges is needed.

This user is defined during the Management Server installation process and is crucial for the smooth operation of the whole system.

Following are the privileges that this user account must have:

- Create GPOs in Active Directory – Each time a policy is created or modified, the Management Server publishes it as a GPO in your Active Directory.
- WMI access to remote machines – Control messages from the Management Server to endpoints are sent over WMI. The user must have the credentials on each of the endpoints for WMI access.

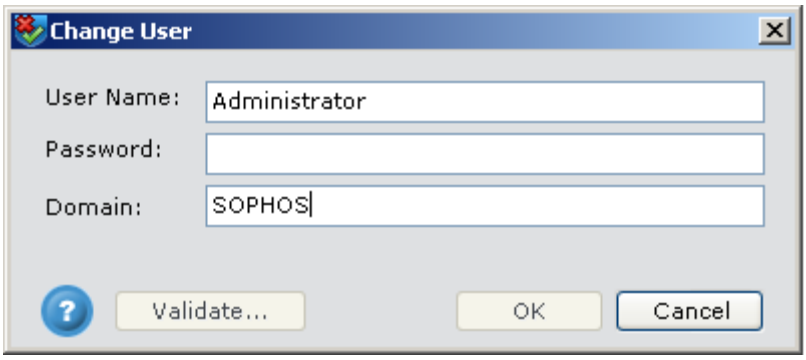
  Note:

  1. We recommend that you use an account with domain administrator privileges on your network, in order to avoid problems.
  2. If at any time you change the "Client Installation Folder" (see below) or choose to deploy policies as .reg files to a folder, you need to make sure this user has full access privileges to these folders (read and write).
  3. If you publish policies only as .reg files, you do not need this user to be authorized to create GPOs in Active Directory.

  Important:

  If you are using Novell, please refer to *Appendix A – Novell eDirectory Synchronization* for instructions.

Change the user whenever necessary by clicking **Change** in the *Domain Credentials* section. The *Change User* window opens:



7.3.1.4.1 Changing a User

1 Enter the credentials (User Name, Password, Domain) of the new user account.

2 You may validate that the user is valid and holds sufficient privileges by clicking **Validate**. Refer to *Server Credentials* for details about this user.

Note: The **Validate** button only validates the existence of the user in your Active Directory. In order for the Management Server to function correctly, you need to make sure all the required privileges are given to the domain user.

7.3.1.5 Users Management

User access to the Management Console is restricted for security reasons. SafeGuard PortProtector does not require its own users and computers database. Instead, credentials are checked using Windows/Active Directory.

Note: If SafeGuard PortProtector is synchronized with Novell eDirectory, only local users on the Management Server can be used.

You may choose one of the following modes of operation:

- ***Single Role (Simple)*** – Using this mode you only restrict access to the Management Console to authorized users. All of them will be able to perform all the tasks in the Console (create policies, read logs, suspend Clients etc.).
- ***Role Based (Advanced)*** – Using this mode you can add an additional level of access control by restricting users to a subset of functions within the Management Console according to their role and permissions and to specific containers of an organization for which they are responsible.

The default mode after installation is – Single Role (Simple).

7.3.1.5.1 Single Role (Simple)

7.3.1.5.1.1 Working with Multiple Management Consoles

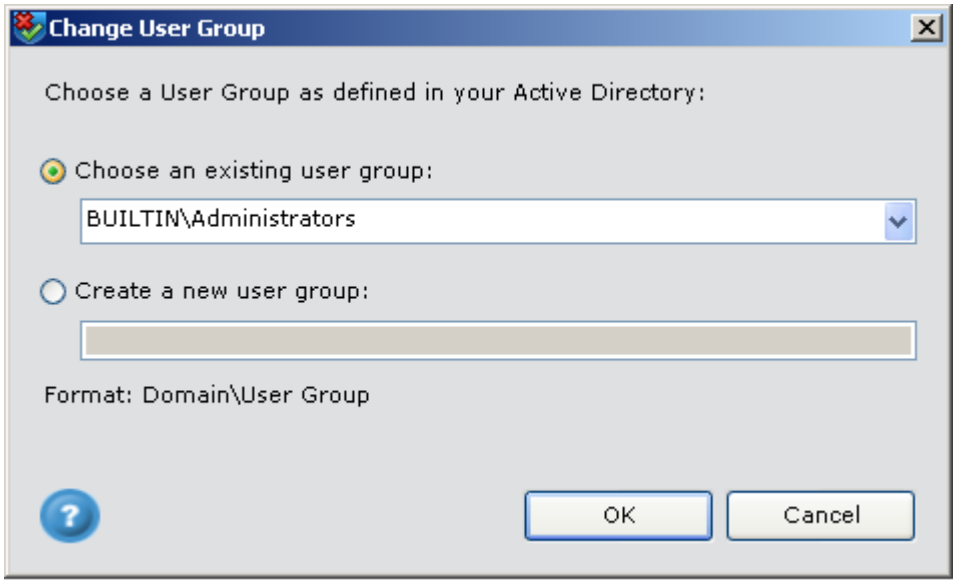
The "Single Role" mode is designed for allowing multiple Management Consoles to access the Management Server, each with his own user and password. This is performed by validating that the user is a member of the user group defined as the "Protector Administrators User Group".

By default, after installing the Management Server this property is set to "BUILTIN\Administrators" which restricts access to the local administrators of the Server machine.

If you are planning on having multiple administrators for SafeGuard PortProtector Management Console, it is recommended that you set here a user group from your Active Directory, and add the appropriate administrators as members of this user group. This is done from the *Change User Group* window.

To open the *Change User Group* window:

In the *Users Management* section, click **Change**. The following window opens:



7.3.1.5.1.2 Changing the SafeGuard PortProtector Administrators User Group

The *Change User Group* window is where you define the appropriate User Group.

To change the User Group:

1 Select one of your existing user groups from the drop-down menu, or create a new user group. When creating a new group, use the following format:
Domain\UserGroup (for example mycompany\administrators).
If you do not enter the domain the new user group is created in the computer hosting the SafeGuard PortProtector Management Server.

2 Click **OK**.

Note: Creation of a new user group is only performed once you have confirmed changes in the Administration window and clicked **OK**.

7.3.1.5.2 Role Based (Advanced)

To determine how the Role Based (Advanced) feature operates, you can configure the following:

- ***Defining Permissions*** – This option enables you to add an additional level of access control by restricting users to a subset of functions within the Management Console.
- ***Defining Domain Partitions*** – This option enables you to partition the containers of an organization so that they are only accessible to the SafeGuard PortProtector Console administrators that are responsible for handling them.

7.3.1.5.2.1 Defining Permissions

Using this mode adds an additional level of access control by restricting users to a subset of functions within the Management Console. You can create multiple user roles and restrict each of them to specific functions in the Console.

For example, you can define a role as "Logs Reviewer" which would restrict users only to the Logs world, without having the ability to view or edit policies. In the same way you can define a role as "Policy Administrators" which would restrict the user to the Policies world, without having the ability to view logs.

Additionally, you can define "Read Only" users who can only view information on the Management Console and cannot perform any changes.

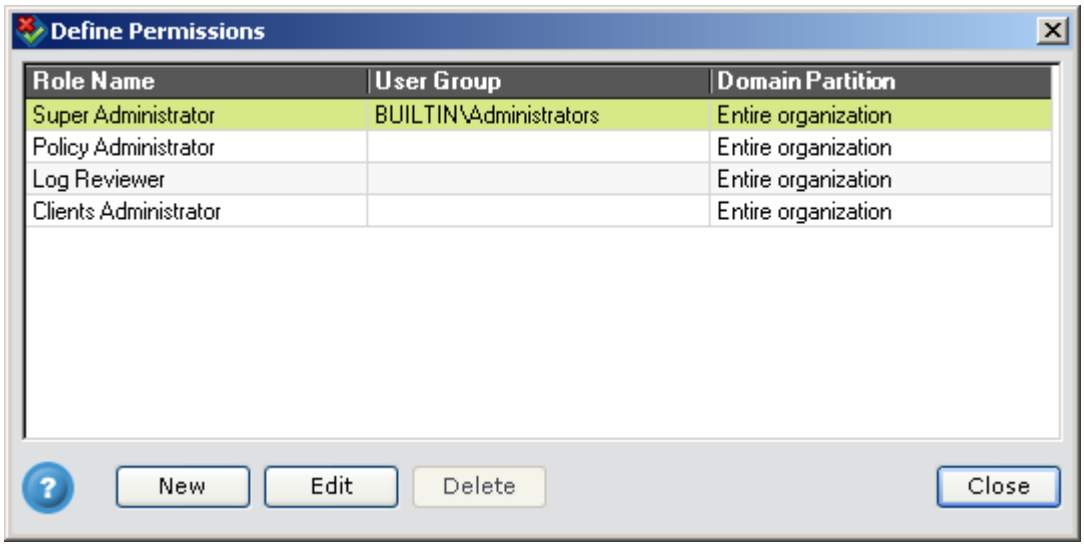
A "role" is actually a set of permissions which are associated with a user group in your Active Directory. When a user tries to access the Management Console, his/her credentials are checked with the domain, and the list of groups of which he/she is a member is retrieved. The user will be authorized to perform the functions which are defined in any of the roles he is associated to.

For example, if the user is both a member of the "Policy Administrators" and "Logs Reviewer" in the example above, he/she is able to access both the Logs and the Policies worlds.

Role definition is defined in the *Define Permissions* window.

To open the *Define Permissions* window:

Click **Define Permissions**. The Define Permissions window opens:



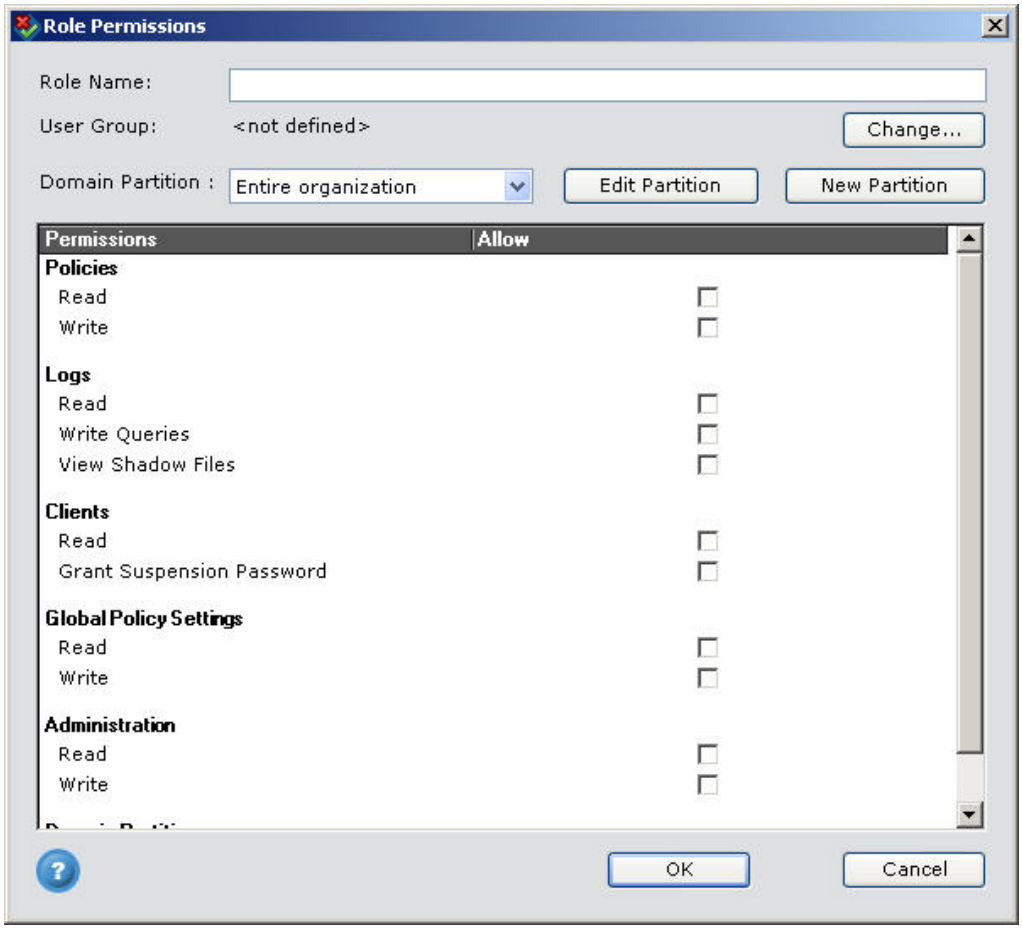
7.3.1.5.2.2 Defining Roles

This window displays a list of the existing roles. In it you can create new roles and edit or delete existing roles. Each row displays a role, the user group with which it is associated and the domain partition to which it has been assigned (See *Defining Domain Partitions*).

The following roles are built into SafeGuard PortProtector: Super administrator, Policy Administrator, Log Reviewer, Client Administrator. If you wish to use any of the last three roles, simply **Edit** them and associate them with a User Group. If you do not wish to use them, you may **Delete** them.

Note: You cannot edit or delete the "Super Administrator" role. This role is preset from the installation of the Management Server and is given all the permissions, including the ability to edit administration settings. The user group associated with this role is derived from the group defined in the "Single Role" mode.

To create a new role, click **New**. To edit an existing role, click **Edit**. The following window opens:



Refer to *Defining Role Permissions* for an explanation of role permission definition.

7.3.1.5.2.3 Defining Role Permissions

To define Role permissions:

1 If this is a new permission, enter the **Role Name**.

2 If you want to define or change the User Group, click **Change**. The *Change User Group* window opens:

3 Refer to *Changing the SafeGuard PortProtector Administrators User Group* for an explanation of this window.

Note: You must select a User Group in order to use a role definition

Note: If you are using Novell, you can only use a local user group on the Management Server.

4 The Domain Partitioning feature enables the partition of the containers of an organization so that they are only accessible to the SafeGuard PortProtector Console administrators that are responsible for handling them. This feature affects almost all aspects of SafeGuard PortProtector's interface, so that only the containers assigned to the Domain Partition associated with a SafeGuard PortProtector user are displayed in the SafeGuard PortProtector console.

Note: The Role permissions define **which administrative actions** each SafeGuard PortProtector administrator can perform and the Domain Partition settings define the **clients on which** they can perform these actions.

To change the partition for this Role permission, select another one in the **Domain Partition** dropdown menu. If you want to define a new Domain Partition, click **New Partition**. To edit an existing Domain Partition, click **Edit Partition**. To change the partition for this Role permission, select another one in the **Domain Partition** dropdown menu.

5 Edit the permissions by checking or un-checking the **Allow** checkboxes. Each checkbox that you allow gives the allowed permission to the user group.

6 Click **OK**.

7.3.1.5.2.4 Defining Domain Partitions

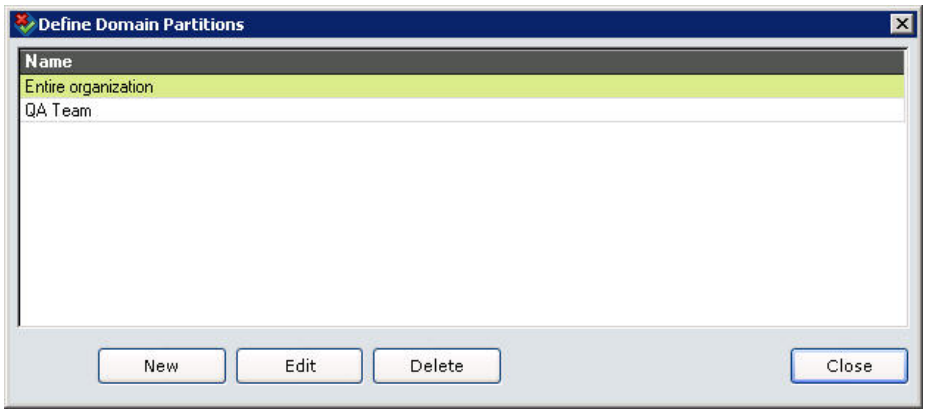
SafeGuard PortProtector's Domain Partitioning enables the partition of the containers of an organization so that they are only accessible to the SafeGuard PortProtector Console administrators that are responsible for handling them. Your organization's domain can be partitioned according to its organizational structure and then different SafeGuard PortProtector administrators can be assigned to each partition.

Note: Domain Partitioning is especially important when using File Shadowing. File Shadowing collects hidden copies of files that are moved to/from external storage devices, and therefore, you may want to restrict access to these sensitive files by defining which administrator is allowed to view a shadowed file according to the file's OU or origin.

Click the **Enable Compartmentalization** checkbox to enable the domain partitioning feature that allows you to divide domain partitions among roles. You can then open the *Define Domain Partitions* window, as described below.

To open the Define Domain Partitions window:

Click **Define Partitions**. The *Define Domain* Partitions window opens:

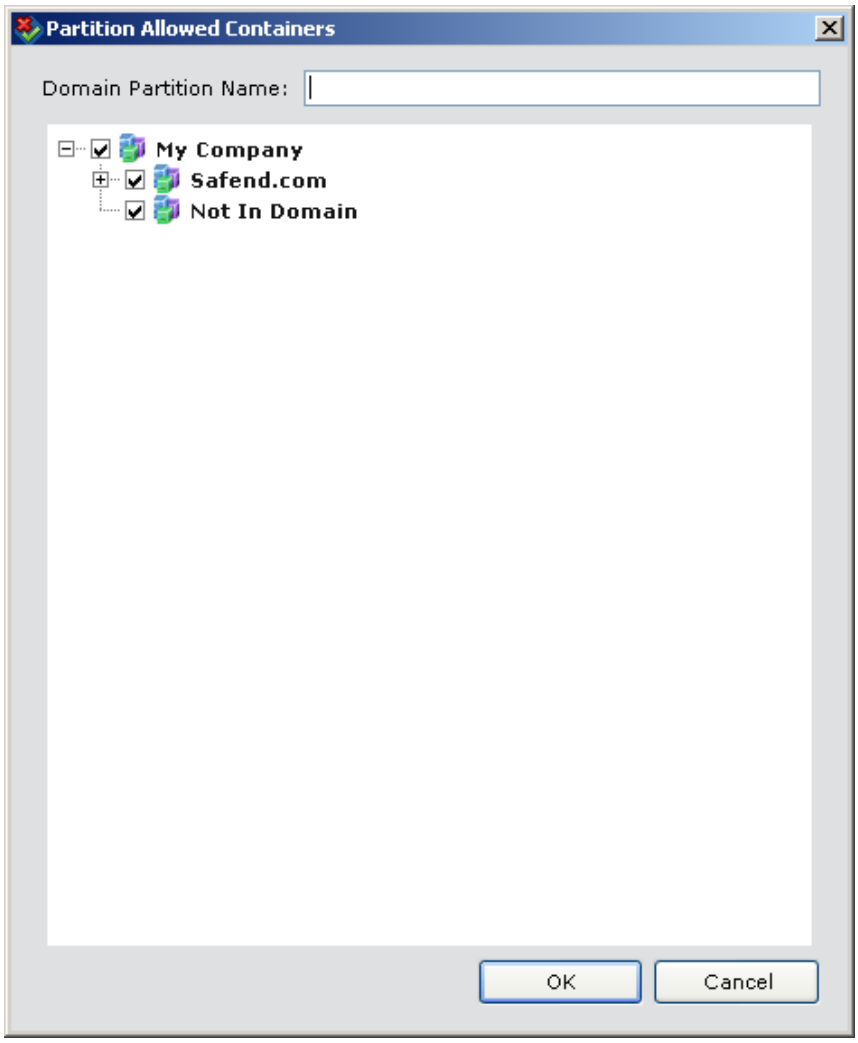


This window displays a list of the existing domain partitions. In it you can create new domain partitions and edit or delete existing domain partitions.

To edit an existing role, click **Edit**.

To create a new domain partition:

1 Click **New**. The following window opens:



2 Enter a name for the domain partition at the top of the window.

3 Check the checkboxes of the containers that you want included in this domain. To do so, you may have to expand the tree to see the containers to be selected.

4 Click **OK**. This Domain Partition is offered for selection in the **Domain Partition** field of the *Role Permissions* window, as described in *Defining Roles*. To associate this partition with a group of users you must associate it with a user role in the *Role Permissions* window.

7.3.1.6 System Language

SafeGuard PortProtector allows you to customize it to your own language. With each new version additional languages are added.

This language affects the following:

- The language for the Management Console menus and buttons
- The language for textual fields in logs
- The language for default end-user messages

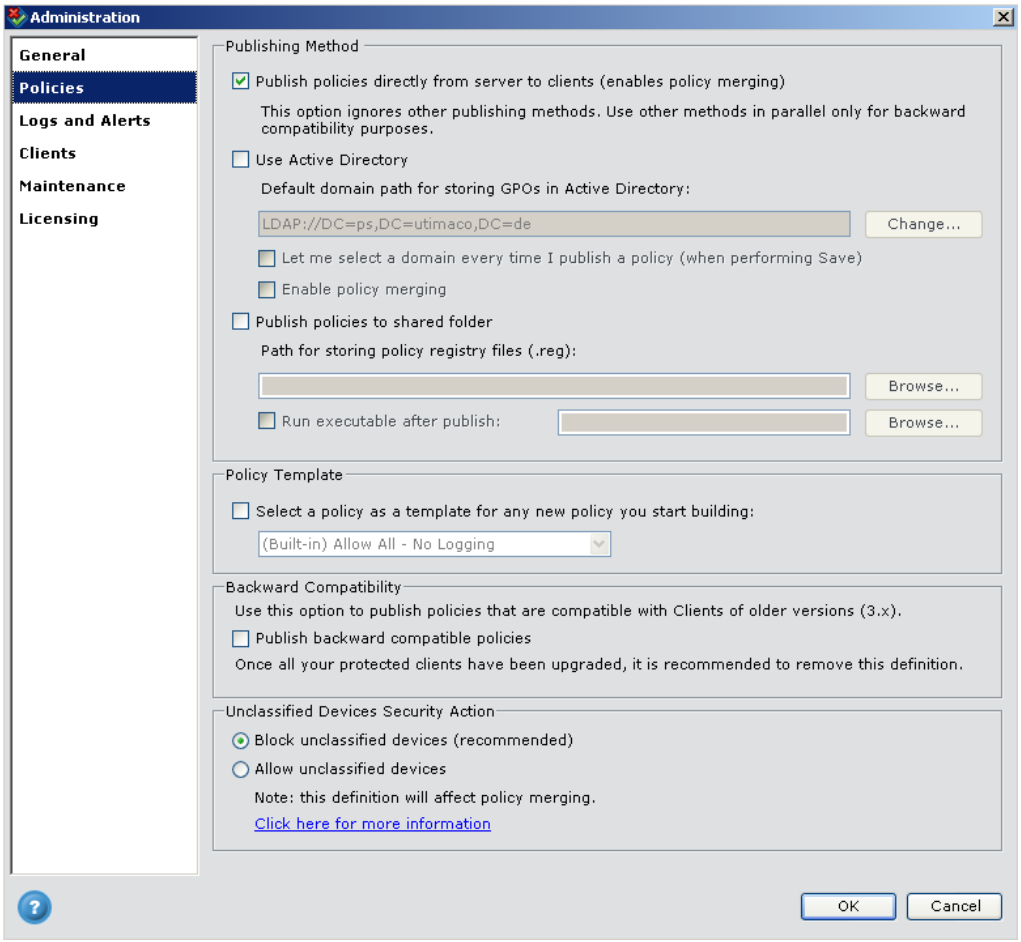
System language is typically defined during the Management Server installation. If you wish to change it after installation, set it here.

Note:

1. After you change language you will need to restart you Management Console for the language change to take affect.
2. You cannot have multiple Consoles in different languages.
3. Log information which was stored before the point of language change is displayed in the previous language.
4. The language for SafeGuard PortProtector Clients is defined during the installation of the Clients (see *SafeGuard PortProtector Installation Guide*).

7.4 Configuring Policies Tab Settings

Policy administration settings are configured in the *Policies* tab in the *Administration* window:


Administration
General
Policies
Logs and Alerts
Clients
Maintenance
Licensing
Publishing Method
Publish policies directly from server to clients (enables policy merging)
This option ignores other publishing methods. Use other methods in parallel only for backward compatibility purposes.
Use Active Directory
Default domain path for storing GPOs in Active Directory:
LDAP://DC=ps,DC=utimaco,DC=de
Change...
Let me select a domain every time I publish a policy (when performing Save)
Enable policy merging
Publish policies to shared folder
Path for storing policy registry files (.reg):
Browse...
Run executable after publish:
Browse...
Policy Template
Select a policy as a template for any new policy you start building:
(Built-in) Allow All - No Logging
Backward Compatibility
Use this option to publish policies that are compatible with Clients of older versions (3.x).
Publish backward compatible policies
Once all your protected clients have been upgraded, it is recommended to remove this definition.
Unclassified Devices Security Action
Block unclassified devices (recommended)
Allow unclassified devices
Note: this definition will affect policy merging.
Click here for more information
OK
Cancel

7.4.1 Policies Settings

The *Policies* tab enables you to configure configuration parameters related to policies in SafeGuard PortProtector. It contains the following sections:

- Publishing Method
- Policy Template
- Backward Compatibility

Note: Whenever you modify any of the settings in this tab you must click **OK** at the bottom of the *Administration* window for the modifications to apply.

7.4.1.1 Publishing Method

SafeGuard PortProtector provides three methods for distributing policies, as discussed in *Chapter 4, Distributing Policies:*

- **Using the Policy Server**: this option enables you to associate policies to organizational objects in the Management Console and to distribute them directly form the Management Server to the Clients.
- **Using Active Directory:** This option uses Active Directory's standard GPO distribution mechanism to distribute policies.
- **Using a Registry File in a Shared Folder:** This option stores registry files in a shared folder from which they can be distributed to SafeGuard PortProtector Clients using a third-party tool, as described on the following page.

The default settings after installation are to publish policies using the Policy Server. If you do indeed use this option, use the other distribution methods additionally only for backward compatibility purposes.

If you select more than one of these options, then SafeGuard PortProtector policy files are copied to the appropriate locations, and any method can be employed to distribute policies to the SafeGuard PortProtector Clients.

If you do not select any of these options then SafeGuard PortProtector policies are stored only in the SafeGuard PortProtector policy database. After you activate one of these options, these policies are then copied to the appropriate locations.

Although most users will typically define their policy distribution method once following installation, you can change these settings whenever you choose. Each time they are changed, the application will regenerate all the policies in the updated locations. Refer to *Chapter 4, Distributing Policies*.

Policy Server

Select the **Publish policies directly from Server to Clients** option to use the Policy Server. This enables you to associate policies to organizational objects in the Management Console and to distribute them directly form the Management Server to the Clients. With this option, if more than one policy is associated with an organizational object all policies are merged (see *Policy Merging* in *Chapter 4, Distributing Policies*). When you use this option, the other options are still selectable. However, use the other distribution methods additionally only for backward compatibility purposes

Active Directory

Select the **Use Active Directory** option to specify that SafeGuard PortProtector policies will be stored as GPOs and then distributed automatically using Microsoft's standard GPO distribution mechanism. In this case, SafeGuard PortProtector automatically creates each policy that you define in the Policies World as a GPO in Active Directory. These policies are then automatically distributed by Active Directory to the Organizational Units to which the GPOs were assigned.

You may refer to *Chapter 4, Distributing Policies* for more details.

Note: If you have previously selected to use the **Distribute policies from a shared folder** option, described on the following page, and later select the **Use Active Directory** option (and de-select the **Shared Folder** option), all existing policies are copied to Active Directory and from this point forward all policies are handled only by Active Directory. This process may take a few moments.

The following parameters are provided when configuring policy distribution in Active Directory:

- **Default domain path for storing GPOs in Active Directory:** This is a read-only field indicating the path where SafeGuard PortProtector GPOs are installed in Active Directory. SafeGuard PortProtector policies are saved as GPOs, which are later assigned to users and computers, as described in *Chapter 4, Distributing Policies*. This field specifies where these GPOs are saved and from where they are taken during distribution.
- **Let me select a domain every time I publish a policy (when performing Save):** If you have a domain forest, check this option to allow you to select the domain to which policies should be published when saved.
- **Enable Policy Merging:** If you select this checkbox, policies applied to Clients will merge with previous policies applied to the Clients to produce the definition that will be applied. Refer to *Policy Merging* in *Chapter 4, Distributing Policies* for an explanation.
  If you later uncheck this checkbox, the last policy applied, and only this policy, will take effect following the next policy update.

Registry Files in a Shared Folder

Check the **Distribute policies from a shared folder** option to specify that SafeGuard PortProtector policies will be stored in a shared folder in registry-file format. These files can then be distributed to the registry of the computers on which the SafeGuard PortProtector Client is installed using a third-party tool. This option does not use Active Directory.

Note: If you used the **Use Active Directory** option, as described on the previous page, and then later you select this option (and de-select the Active Directory option), all existing policies are copied to the specified shared folder and from this point all policies are only handled as registry files in a shared folder. This process may take a few moments.

To define that policies are published as registry files:

1 Check Publish policies to a shared folder.

2 In the path for storing policy registry files (.reg) field, enter or browse to the shared folder in which these registry files will be stored.

Note: If you are using a Management Console that is not on the same machine as the Management Server, the path you select will be relative to the Server, not the Console.

3 Make sure that:

4 The specified folder is accessible by your third-party tool in order for it to distribute policies to SafeGuard PortProtector Clients.

5 The specified folder is accessible (read and write) by the user account you have specified in *Server Domain Credentials* above in order for the Management Server to be able to publish policies to this folder.

6 Optionally – You can check **Run executable after publish** (see below)

When this option is used, SafeGuard PortProtector generates two copies of the registry file, one suitable for computers (for example: **MyPolicy(MACHINE).reg**) and one suitable for users (for example: named **MyPolicy(USER).reg**).

You may refer to *Chapter 4, Distributing Policies* for more details.

7.4.1.1.1 Run Executable after Publish

You may wish to automate the process in which policies are distributed by a third party tool (i.e. SMS, Novell eDirectory) after editing/creating policies.

This option enables automatic activation of an executable whenever policies are published as .reg files. This executable then performs the functions needed to reflect the change of policy to the third-party tool.

For API and details of the interface parameters please contact Support: mailto:support@sophos.com.

7.4.1.2 Policy Template

Each time you create a new policy, default values appear for security options (ports, devices etc.) and for settings (end-user messages, logs interval etc.).

With this option you can choose to set any of the policies you have already defined as a template which replaces the default when creating new policies. This is useful when you have specific settings you prefer to start from rather than the default.

To select a policy a s a template:

Check the checkbox and select the policy of your choice from the drop-down menu.

Note: This option is disabled until you create at least one policy.

7.4.1.3 Backward Compatibility

If you have upgraded your SafeGuard PortProtector Management Server from an earlier version (3.1 or lower), but have not yet upgraded your Clients, you may want policies published by this version to be compatible with Clients of the older version.

Once all the SafeGuard PortProtector Clients in your network have been upgraded, it is recommended that you remove this definition.

To publish backward compatible policies:

In the *Backward Compatibility* section, click the checkbox. Policies published from this moment on will be compatible with earlier Client versions.

7.4.1.4 Allowing / Blocking Access to Unclassified Devices

Unclassified devices are devices that cannot be classified by SafeGuard PortProtector into one of the device categories described in *Appendix B - Supported Device Types*.

SafeGuard PortProtector is generally able to classify almost any device. However, some devices do not fit into any of the built-in device categories or do not employ the proper mechanisms that enable their classification by SafeGuard PortProtector, or by the operating system itself. For this purpose, SafeGuard PortProtector provides special handling for unclassified devices, as described in this section.

Typically, an organization does not want unknown (unclassified) devices to connect through the restricted ports on its endpoints, as this may present a security breach.

However, during the initial deployment stages of SafeGuard PortProtector, an organization may want to temporarily allow access by unclassified devices. This will enable a smooth transition into a more secure manner of work, without prematurely blocking unclassified devices before they can be added to a policy that specifically allows them.

Therefore, an organization may initially **allow** unclassified devices to continue to access the organizations ports, while each access is logged. The administrator can then query the SafeGuard PortProtector logs to see which unclassified devices are being used and then to allow those specific devices in a policy.

After this permissive approach has been used during initial deployment and after the administrator has defined the unclassified devices that should be approved in one or more policies, it is recommended to start blocking unclassified devices.

Note: Setting unclassified devices as **Allowed** affects the way policies are merged, so that the most restrictive Device Control definitions of all merged policies that apply to the same OU take effect. You may refer to *Policy Merging When Unclassified Devices are Allowed* for more information.

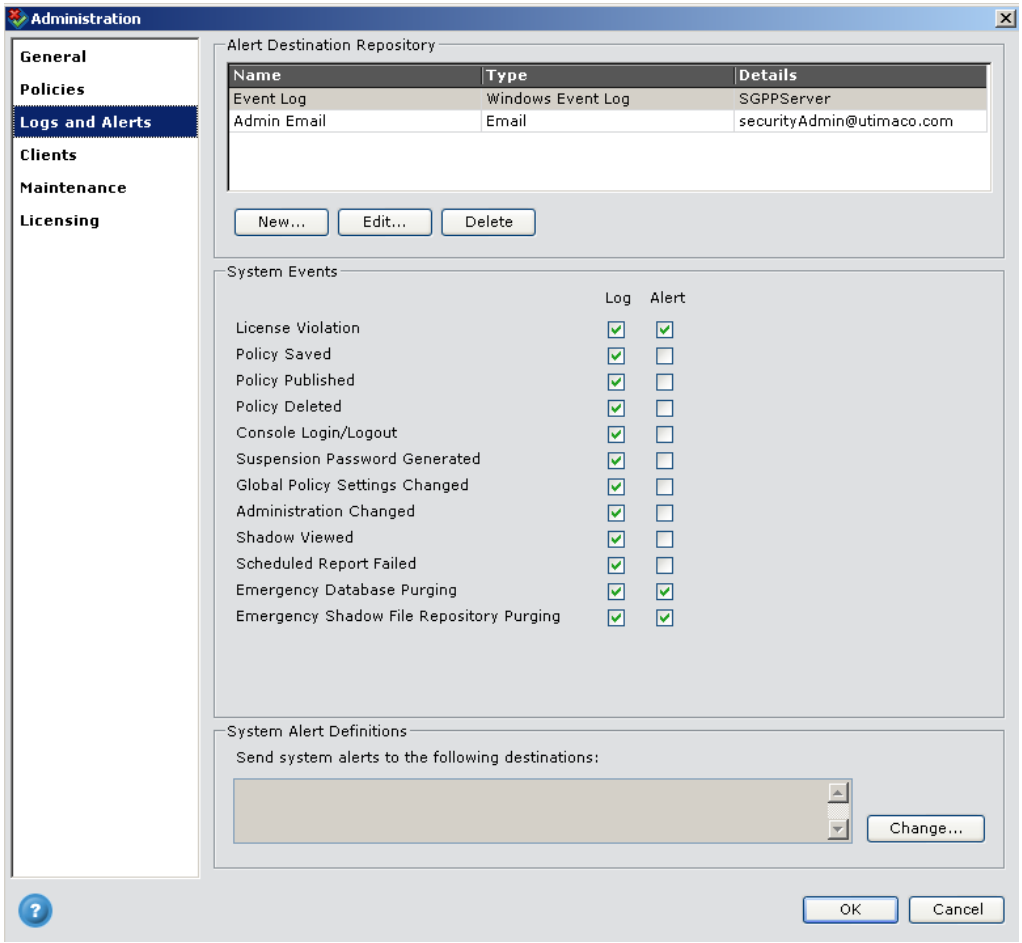
Note: When unclassified devices are defined as **Allowed** in the *Policies* page of the *Administration* window, it will affect the *Device Control* window in the *General* tab of the *Policy* window. The *Device Control* window will show **Allow** ( ) in the **Devices Not Approved in Device Types or White List** area for *Unclassified Devices* at the bottom of the window. This indicates that unclassified devices are allowed and that Device Control policy merging has been affected.

To define the security actions for unclassified devices:

In the *Unclassified Devices Security actions* section, select either the **Block Unclassified Devices** (**recommended**) option or the **Allow Unclassified Devices** option, as described above.

7.5 Configuring Logs and Alerts Tab Settings

Log and alert definitions and destinations are configured in the *Logs and Alerts* tab in the *Administration* window:



7.5.1 Log and Alert Settings

The *Logs and Alerts* tab enables you to configure the Alert Destination Repository, as well as log and alert definitions and alert destinations for Management Server events. It contains the following sections:

- *Alert Destination Repository*
- *System Events*
- *System Alert*

Note: Whenever you modify any of the settings in this tab you must click **OK** at the bottom of the *Administration* window for the modifications to apply.

7.5.1.1 Alert Destination Repository

This is where you view, edit, define and delete the destinations available in your network for sending alerts. A destination is the address to which alerts are sent.

The list of address destinations is called the *Alert Destination Repository*. Once you have created the repository, you can select from it the desired destinations to be used for System alerts (see *System Alert Definitions*), for policy-specific alert settings (see *Defining Alert Settings* in *Chapter 3, Defining Policies*) and for global policy alert settings (see *Step 9: Define Global Policy Settings* in *Chapter 3, Defining Policies*).

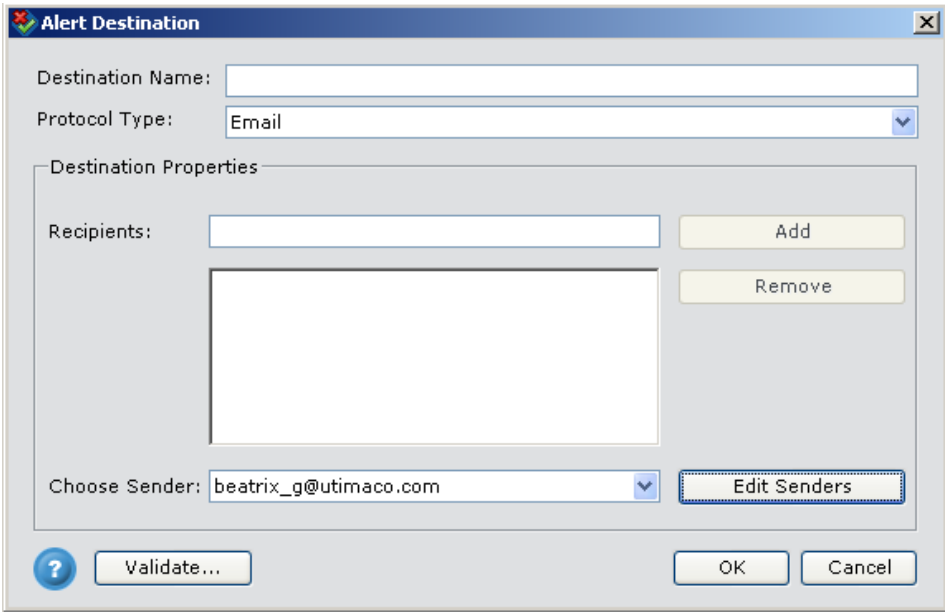
Destinations can be of multiple protocol types including:

- **Email** – send to a single/multiple address/es
- **SNMP** – generate an SNMP trap to be sent to network monitoring systems (i.e. HP Openview, IBM Tivolli)
- **Windows Event Log** – insert a log entry to a specific computer event log
- **Executable** – run an executable which will perform any kind of action with the alert information
- **Syslog** send a message to a syslog compatible server.

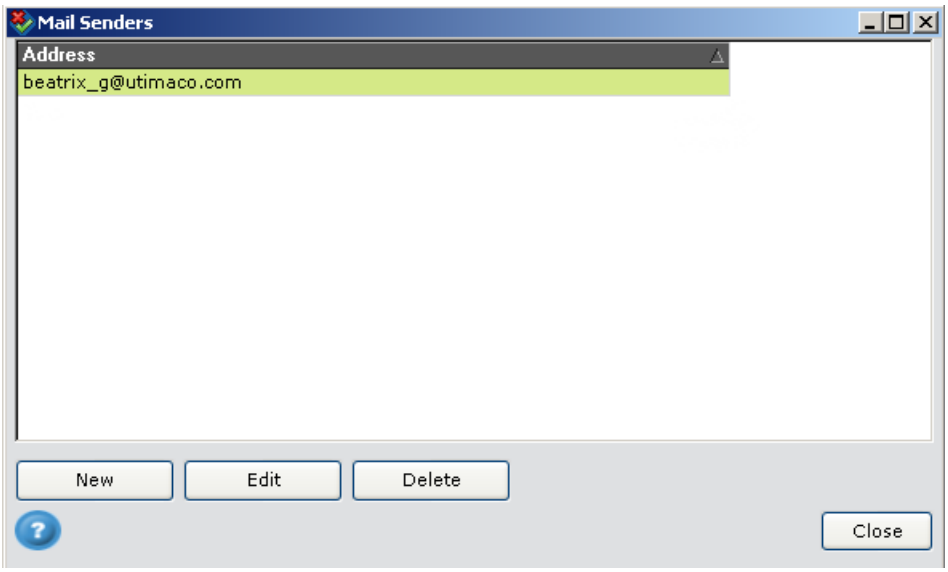
Alert destinations are set in the *Alert Destination* window.

To open the *Alert Destination* window:

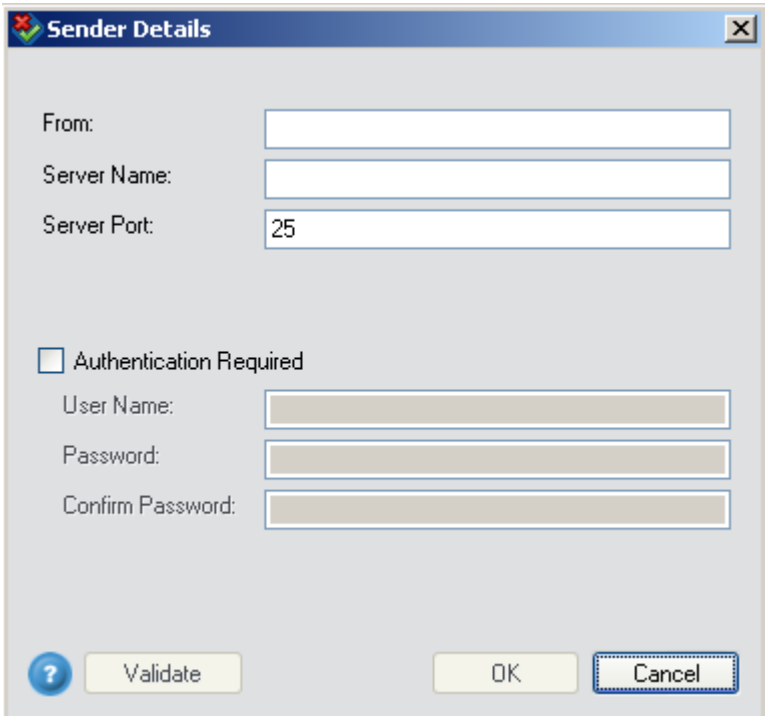
1 In the *Alert Destination Repository* section, click **New**. The *Alert Destination* window appears:



2 To define a new send, click the **Edit Senders** button to display the following window:



You can click the **New** button to add a new sender in the following window.



7.5.1.2 Defining a New Mail Sender

Following are the properties required for setting a new mail sender:

- **From** – this field appears in the **From** fields of the emails that are sent.
- **Server Name** – the host name of your outgoing email server (SMTP). You can also type an IP address.
- **Server Port** – the TCP port for sending email. This is typically port 25. If you are using secure email, then the port may be different.
- **Authentication (Optional)** – If your outgoing email server requires authentication, enter the following fields as well:
- **User Name**
- **Password**

7.5.1.3 Setting an Alert Destination

Following are the properties required for each of the protocol types:

- Email
- **Recipients** – type in a valid email address to which email will be sent. You can also type several addresses, comma/semicolon separated. Select **add** to add the mail address you typed to the recipients list.
- In the **Choose Sender** field, select the email address to be specified as the sender from the dropdown menu. The dropdown menu lists the senders that were entered previously in SafeGuard PortProtector either in this window or in the *Schedule Report* window. You can also click the **Edit Sender** button to define a new sender, edit an existing sender or delete a sender.

  Note:

  The dropdown menu in the *Alert Destination* window lists the senders that were entered previously in SafeGuard PortProtector either through this window or in the *Schedule Report* window.
- SNMP
- **Server Name** – the host name of your SNMP server. You can also type an IP address.
- **Server Port** - the TCP port for sending SNMP traps. This is typically port 162.
- Windows Event Log
- **Host Name** – the host name on which to write Windows event logs. You can also type an IP address.

- Executable
- Path to executable – the path to an executable to be launched by an alert, if desired.

For details of *the* API parameters please contact Support at mailto:support@utimaco.de.

To add an alert destination:

1 In this window, enter the required details and click **OK**.

2 After you click **OK**, the system validates the destination you have entered. If not valid, check your settings and try again.

3 You can also click **Validate** to perform manual validation.

Once you have created the Alert Destination Repository, you can select from it the desired destinations to be used for System alerts (see *System Alert Definitions*), for policy-specific alert settings (see *Defining Alert Settings* in *Chapter 3, Defining Policies*) and for global policy alert settings (see *Step 9: Define Global Policy Settings* in *Chapter 3, Defining Policies*).

Note: If you change the properties of a destination, it will affect all alerts that use this destination – system alerts policy-specific alerts and global policy alert settings.

7.5.1.4 System Events

System events track events generated by the Management Server and actions performed in Management Consoles. In this section you define which events are logged (and can be viewed in Server Logs) and which also generate an alert.

System events include:

- License Violation
- Policy Saved
- Policy Published
- Policy Deleted
- Console Login/Logout
- Suspend Password Granted
- Global Policy Changed
- Server Configuration Changed
- Shadow Viewed
- Scheduled Report Failed
- Emergency Database purging
- Emergency Shadow File Repository purging

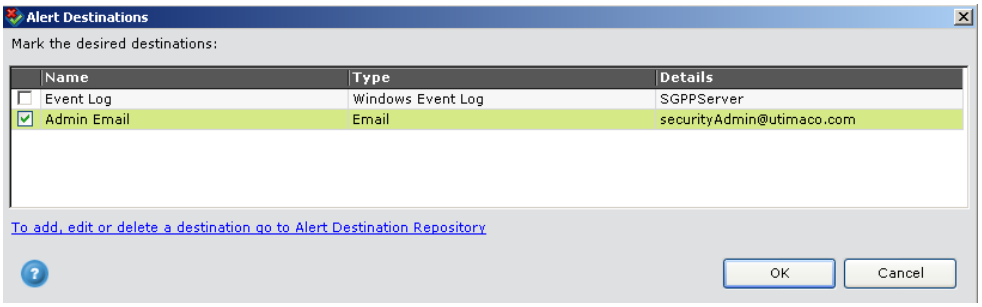
By default all events are logged. You can remove some of the logs or set events for which you would like the Management Server also to send an alert.

7.5.1.5 System Alert Definitions

Select here the destinations to which the Management Server send alerts generated as a result of systems events. Alerts are sent only for event types you have chosen in the previous section.

To add/remove destinations:

1 Click **Change**. The *Alert Destinations* window opens, displaying all available destinations defined in the Alert Destination Repository (refer to Alert Destination Repository in *Chapter 7, Administration*).

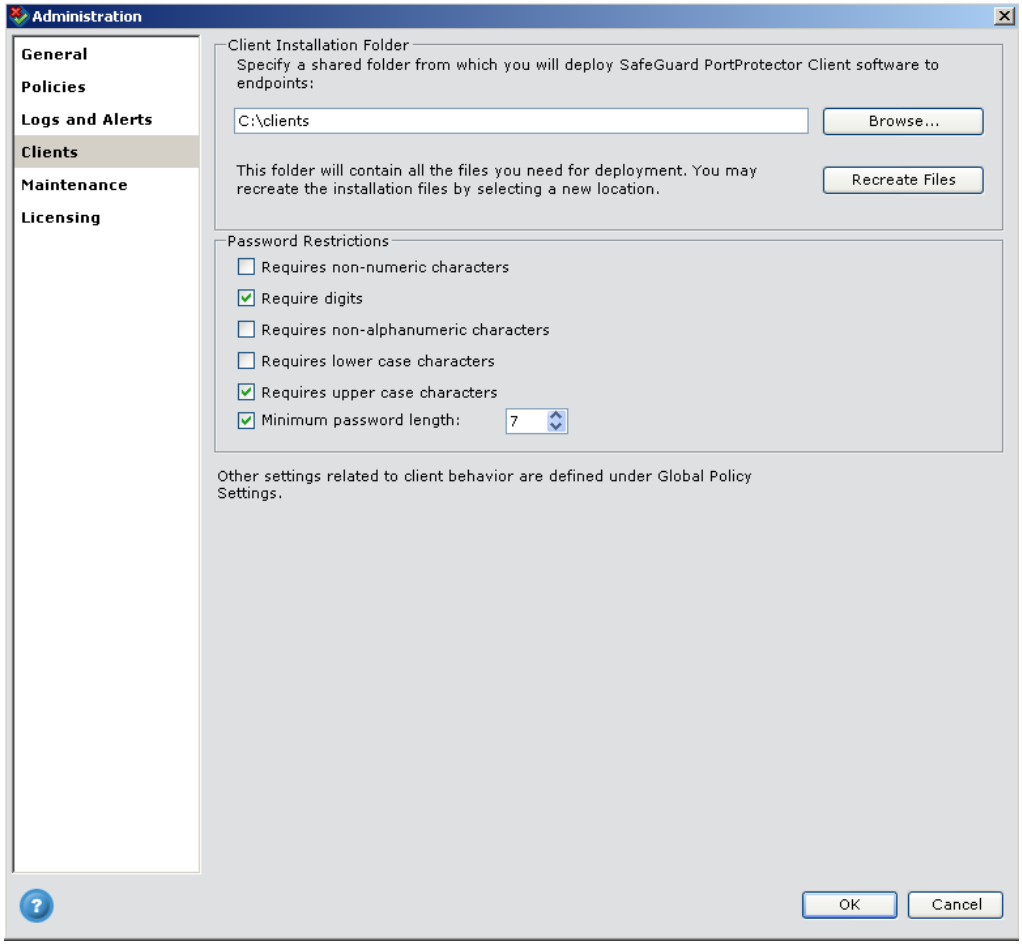


2 Select or de-select the required destinations and click **OK**.

Note: To add, edit or delete a destination, refer to Alert Destination Repository in *Chapter 7, Administration.*

7.6 Configuring Clients Tab Settings

Client administration settings are defined in the *Clients* tab in the *Administration* window:



7.6.1 Client Settings

The *Clients* tab enables you to configure the folder in which you would like to store the Client installation files in the *Client installation* folder section and to define the criteria for using passwords in SafeGuard PortProtector in the *Password Restrictions* section.

Note: Additional Client settings such as uninstall password, log interval and Client visibility settings are set in the *Global Policy Settings* window accessible from the *Tools* menu and described in *Step 9: Define Global Policy Settings* in *Chapter 3, Defining Policies.*

7.6.1.1 Client installation folder

This is the folder to which the Management Server exports the files needed for installing SafeGuard PortProtector Clients on endpoints. In order to deploy Clients, you need to define a folder for the installation files to be created.

This folder should typically be a network path accessible for deploying software to endpoints.

Note: Whenever you modify any of the settings in this tab you must click **OK** at the bottom of the *Administration* window for the modifications to apply.

To set the shared folder for Client installation files:

1 Click **Browse**.

2 Select a network path for the shared folder and click **OK**.

3 Once you set a new path, the Server will copy the following files to the new path:

- SafeGuardPortProtectorClient.msi
- SafeGuardPortProtectorClient.exe
- ClientConfig.scc

4 You can also click **Recreate Files** at any time to recreate files if for some reason they were damaged.

Please refer to the SafeGuard PortProtector Installation Guide for instruction regarding Client deployment.

Note: Additional Client settings such as uninstall password, log interval and Client visibility settings are set in the *Global Policy Settings* window accessible from the *Tools* menu and described in *Step 9: Define Global Policy Settings* in *Chapter 3, Defining Policies.*

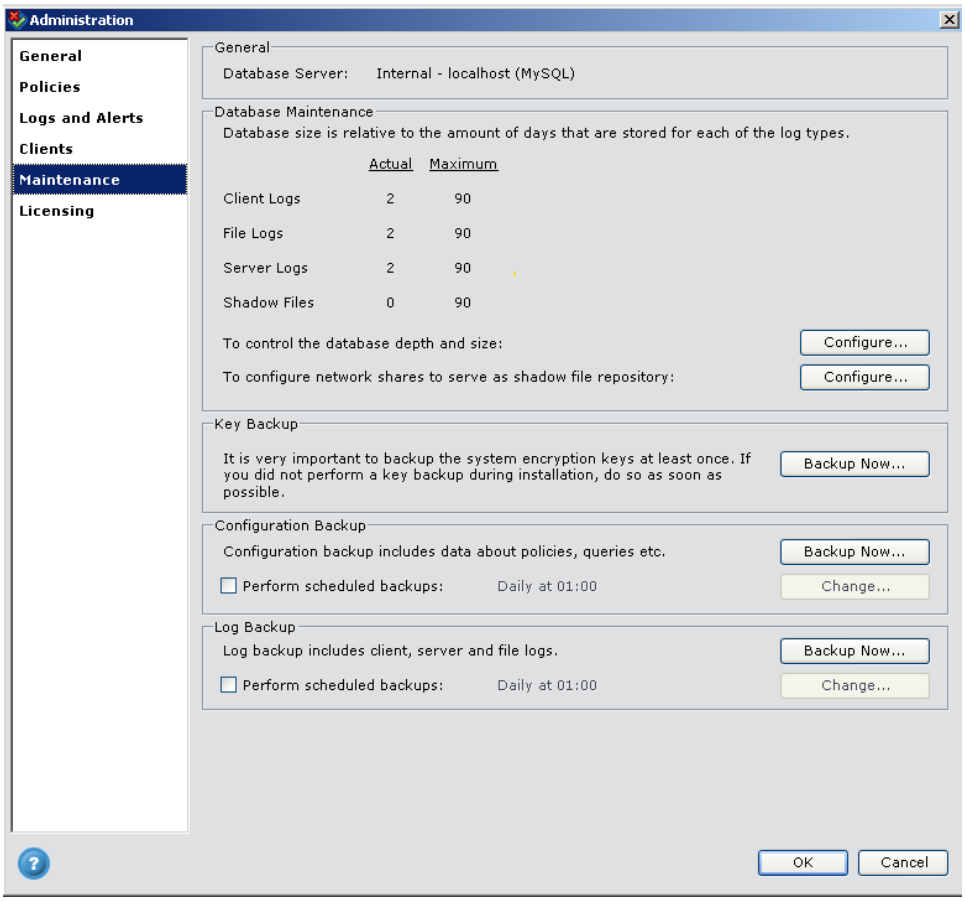
7.6.1.2 Password Restrictions

SafeGuard PortProtector provides a number of places where its operation is password protected, such as: when uninstalling a client, when using its Access Secure Data utility and when accessing the Administration on a SafeGuard PortProtector client.

Check the relevant options in this area to control the characteristics of the passwords that can be used in SafeGuard PortProtector, such as the type and quantity of characters and the maximum password length. You can select any combination of the provided options in this section of the window.

7.7 Configuring Maintenance Tab Settings

Maintenance settings are defined in the *Maintenance* tab in the *Administration* window:



7.7.1 Maintenance Settings

From the *Maintenance* tab you can perform various system maintenance activities. These allow you to define database maintenance, encryption key backup, configuration backup and log backup settings. It contains the following sections:

- *General*
- *Database Maintenance*
- *System Backup*
- *Log Backup*

Note: Whenever you modify any of the settings *in this* tab you must click **OK** at the bottom of the *Administration* window for the modifications to apply.

7.7.1.1 General

This section displays the name of the database server and whether it is the SafeGuard PortProtector internal MySQL server or an external MS SQL server.

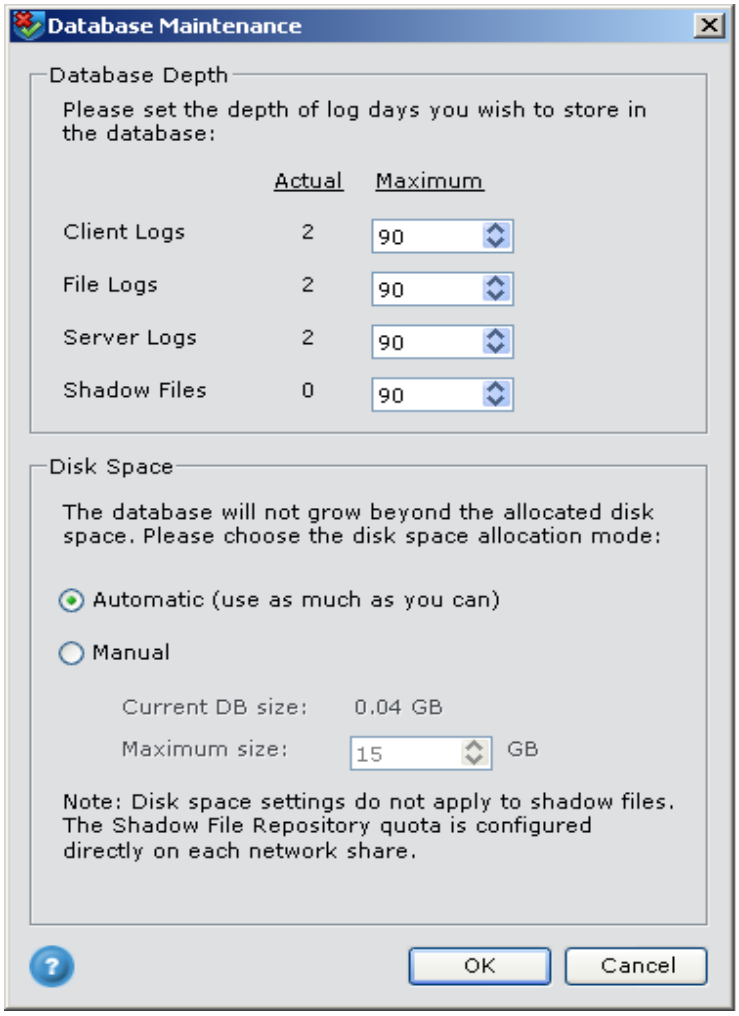
7.7.1.2 Database Maintenance

This section deals with managing the database by means of setting the number of log days (depth) you wish to store for each type of log, and defining the disk space allocated to the database, in which logs comprise the bulk of the disk space. The purpose of the database management is to allow you to save the depth you require, or as close to it as possible. This is done in the *Database Maintenance* window, as described in the Defining Database Maintenance Settings section.

In addition, this section allows you to configure the network shares to be used as the central repository for shadowed files, as described in Defining File Shadowing Network Shares section.

To open the *Database Maintenance* window:

In the *Database Maintenance* section, next to the **To control the database depth and size** field click **Configure**. The *Database Maintenance* window opens:



7.7.1.2.1 Defining Database Maintenance Settings

The *Database Maintenance* window includes two sections:

- **Database Depth**: displays the actual number of days currently stored for each log type and allows you to set the required (maximum) number of storing days for each log type.
- **Disk Space**: allows you to allocate database disk space automatically or manually. By default, disk space is managed automatically and aims to avail you of the requested depth. We recommend that you allocate disk space manually only if you have another application running on the same server whose disk space usage is of a rapidly-growing nature.

Note: When using an external database this section does not appear as in this case disk space is not managed by SafeGuard PortProtector.

To configure database maintenance settings:

1 In the *Database Depth* section, set the number of days you wish to store for each log type – Client logs, File logs, Server logs and Shadow Files.

2 Click the appropriate radio button in the *Disk Space* section to select whether you wish disk space to be allocated automatically or whether you prefer manual disk space allocation (current database size is displayed).

Note: When using an external database this section does not appear as in this case disk space is not managed by SafeGuard PortProtector.

3 If you selected manual allocation of disk space, set the maximum disk space to be used by the database.

4 Click **OK**. Log depth and database size will now conform to these settings.

Note: When using the SafeGuard PortProtector internal database, when disk space is too low to hold the required database depth, an emergency purge is performed in which oldest records are deleted in order to free disk space. If this happens, a message appears in the *Database Maintenance window* and in the *Database* section of the Home World informing you that the database does not currently hold the required depth due to low disk space and that you should allocate additional disk space or change depth requirements.

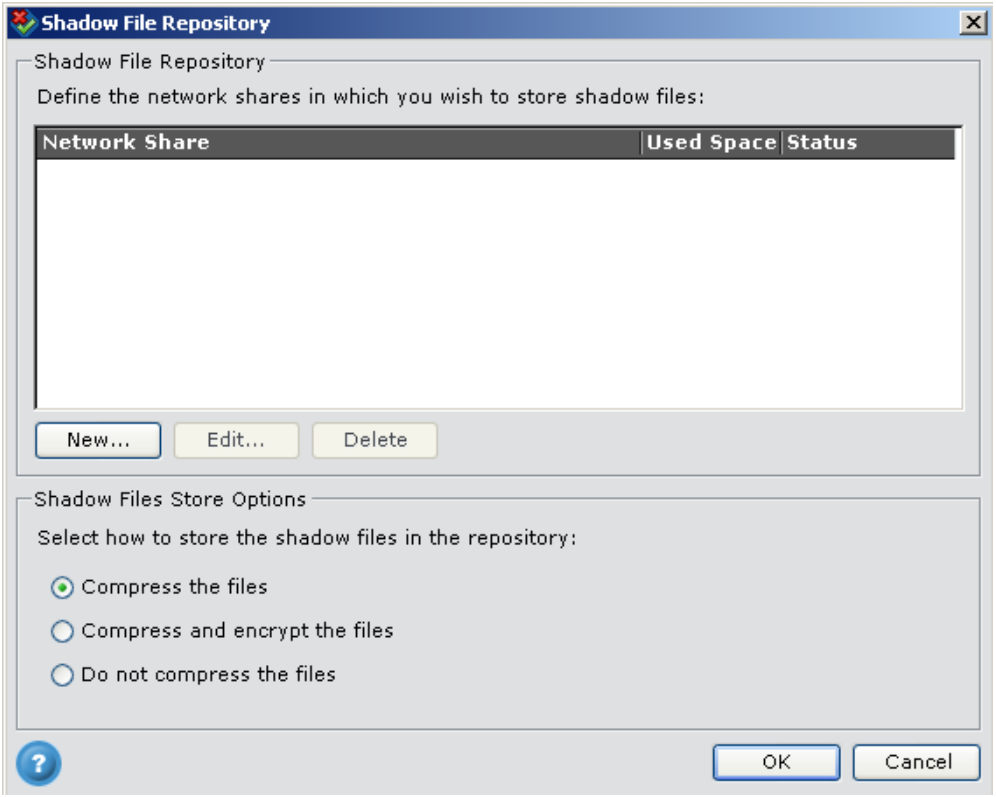
7.7.1.3 Defining File Shadowing Network Shares

This section describes how to configure the network shares to be used as the central repository for shadowed files. One or more network shares can be defined by an administrator as the Shadowed files central repository. If multiple network shares are defined, then a load balancing algorithm is used to verify that utilization is distributed evenly among all the shares.

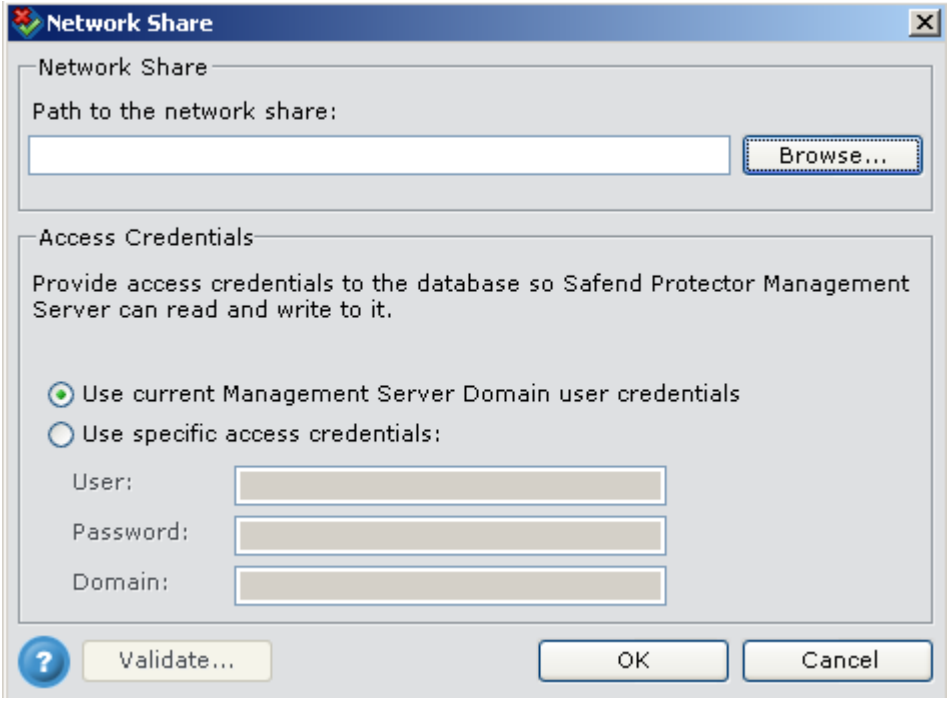
Note: Much like the logging mechanism, shadowed files are cached on the local protected machine until they can be relayed to a server. See Defining File Shadowing Settings for more information.

To configure the File Shadowing network shares:

1 In the **Database Maintenance** area, to the right of the **To configure network shares as shadow file repository** field, click **Configure**. The following window is displayed listing the network shares already defined as shadowed files repository.



2 Click the **New** button to define a new network share. The following window is displayed:



3 Click **Browse** to display a window in which you can specify the path to this network share.

4 Select this path and then click the **Make New Folder**. A window is displayed requesting the credentials to access this folder.

5 Enter the credentials and click **Validate** to test access to the folder. Click **OK**.

Note: If multiple network shares are defined, then a load balancing algorithm is used to verify that utilization is distributed evenly among all the shares and that seamless failover can occur in cases of failure when accessing one of the shares.

6 You can compress and encrypt the files in the repository by selecting one of the following options. Only Authorized administrators are able to access encrypted files from the management console.

- Compress the files
- Compress and encrypt the files
- Do not compress the files

7 The added network share is defined as Active by default in the *Shadow File Repository*. You can right-click on it in the window to select the **Deactivate** option. Deactivating a network share means that shadowed files are no longer written to it. However, files that are already in the network share can still be viewed by an authorized administrator.

You can delete a network share by selecting it in the in the S*hadow File Repository* and clicking **Delete**. If you delete a network share, then **its files** can no longer be viewed by an authorized administrator.

7.7.1.4 System Backup

Backing up your system is recommended, so that your existing system can be restored, should this be necessary in cases when you need to re-install the Management Server. System backup includes data about policies, Queries, Server keys, etc.

To perform schedules backup:

In the *System Backup* section, check the **Perform scheduled backups** checkbox. System backup will be performed at the scheduled times (the upcoming scheduled time is displayed).

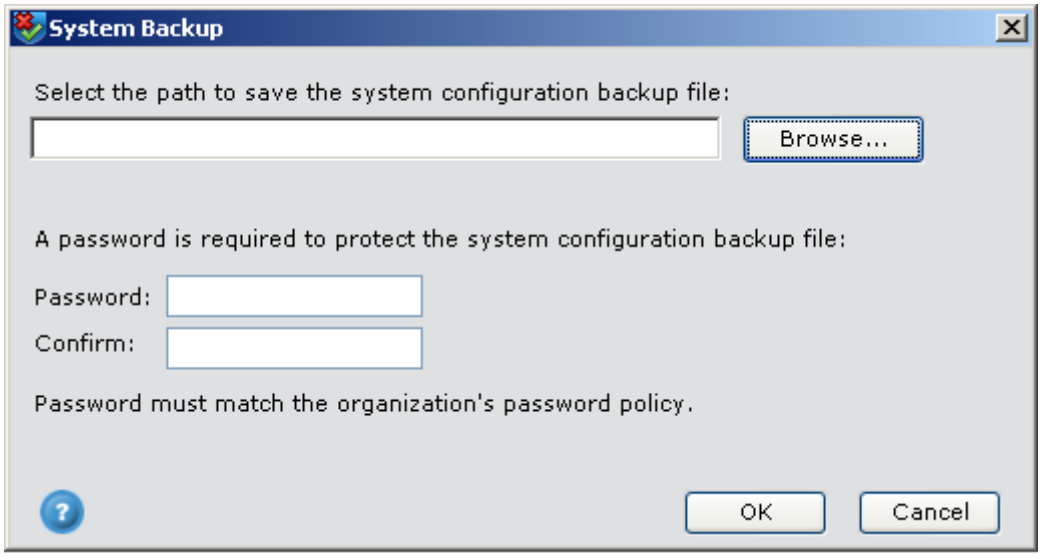
If you wish to change the system backup schedule, you may do so. See *Scheduling System Backup*.

7.7.1.4.1 Backing Up the System

In order to backup the system, you are required to set a password for the backup file. This password will be required when you try to use this backup to restore your Management Server.

To backup the System:

1 Click Backup Now. The System Backup dialog box is displayed.



2 Select a path in which to save the System configuration backup file.

3 Set a password for the backup file and conform it.

4 Click **OK**. The backup keys are saved.

Note:

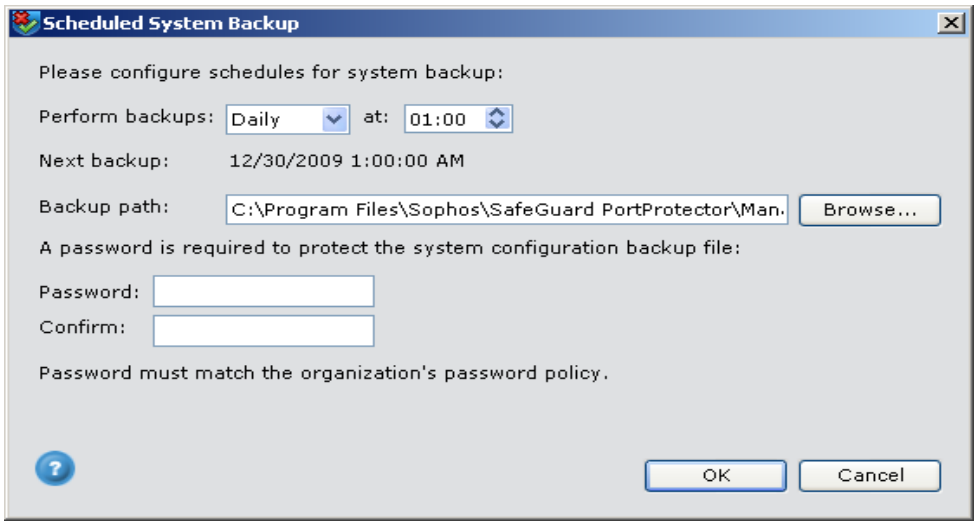
1. You can backup the System at any point in time. It is recommended to store several backups on different machines and sites.
2. If you forget the password you have used, just perform the backup again and use a new password.

7.7.1.4.2 Scheduling System Backup

You can configure the schedule for System Backup.

To configure the System backup Schedule:

1 Click **Change**. The Schedule System Backup dialog box is displayed.



2 Set **Perform backups** interval (*Daily*, *Weekly*, *Monthly*) and time.

3 Click **Browse** to select the backup path.

4 Enter a password and confirm it.

5 Click **OK**. The configuration backup schedule is now set. Configuration backup files are saved under the following name convention: `ConfigurationBackup01JAN2009_2359.SCB`, where 01Jan2009_2359 are the time and date. The new backup file does not overwrite the current file, so that two backup files are always available.

7.7.1.5 Log Backup

Note: When using an external database this section does not appear as in this case backup is not managed by SafeGuard PortProtector.

In much the same way as for your configuration, you can also backup you logs. This is includes Clients logs, Server logs and File logs. You may perform ad-hoc backup at any time, or schedule predefined backups.

To perform backup at any time:

1 In the *Log Backup* section, click **Backup Now**. The *Select Log Backup File* window opens.

2 Select the desired path, enter the desired file name and click **Save**. Logs are backed up.

You also have the option of performing scheduled log backup at regular, predefined intervals.

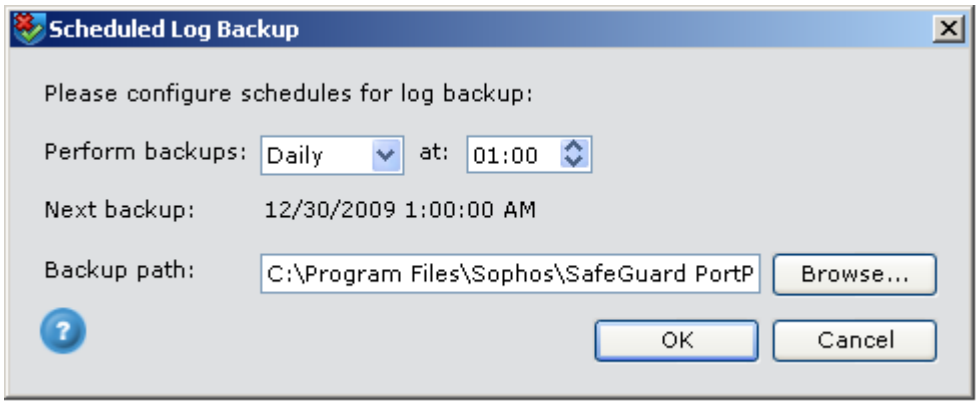
To perform scheduled backup:

In the *Log Backup* section, check the **Perform scheduled backup** checkbox. Log backup will be performed at the scheduled times (the upcoming schedule time is displayed).

If you wish to change the log backup schedule, you may do so.

To schedule log backup:

In the *Log Backup* section, click **Change**. The **Log Backup Schedule** window opens:



7.7.1.5.1 Scheduling Log Backup

In this window you can set the interval (daily, weekly or monthly) and the time for your scheduled log backup, and the backup path.

To set backup parameters:

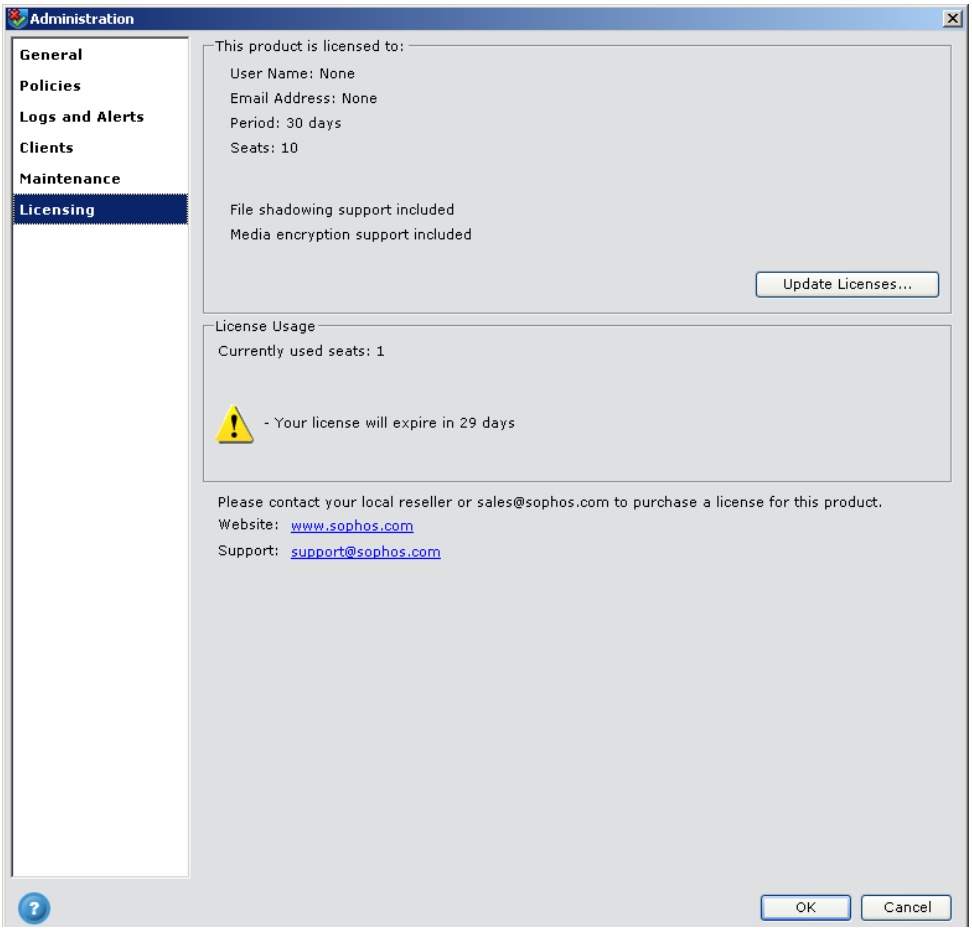
1 Set **Perform backups** interval and time.

2 Click **Browse** to select the backup path.

3 Click **OK**. The log backup schedule is now set. Log backup files are saved under the following name convention: `LogsBackup01JAN2006_2359.SLB`, where 01Jan2006_2359 are the time and date. The new backup file does not overwrite the current file, so that two backup files are always available.

7.8 Configuring Licensing Tab Settings

Licensing details are displayed, as well as updated, in the *Licensing* tab in the *Administration* window:



Note: SafeGuard PortProtector provides various additional features that are activated by license. These additional features are listed under **This product is licensed to**.

7.8.1 Licensing Settings

The first time you open the application, a window opens to alert you that the installation will expire in 30 days. During this period you should contact Utimaco Safeware AG – a member of the Sophos Group and purchase a license for the product.

If the license has already expired, a message is displayed and you cannot perform any operations in the system until a valid license key is entered.

The *Administration* window *Licensing* tab displays licensing details for SafeGuard PortProtector. This license can be updated, as necessary. The *Licensing* tab contains the following sections:

- *License Details*
- *License Usage*

Note: Whenever you modify any of the settings in this tab you must click **OK** at the bottom of the *Administration* window for the modifications to apply.

7.8.1.1 License Details (this product is licensed to)

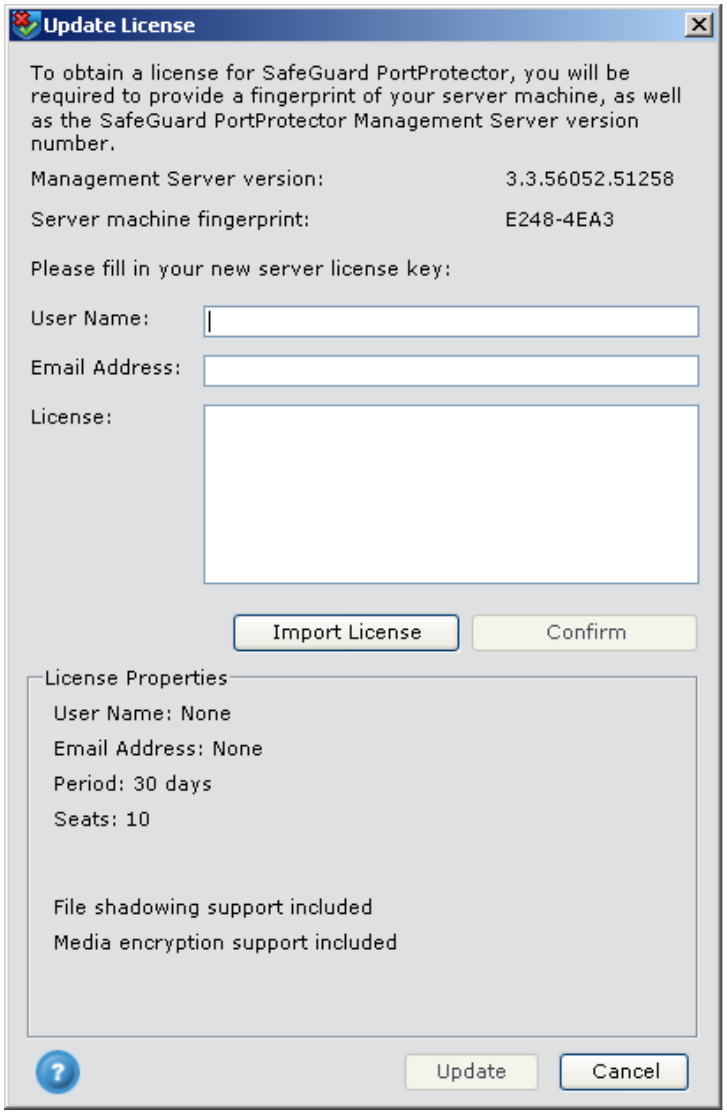
- **User Name:** Name that was used during the procurement of the product.
- **Email Address:** Email address that was used for sending the license key.
- **Time Period:** Number of days given in the license.
- **Seats:** Number of allowed licensed Client stations.
- **Included Abilities:** add-on features or products included in the license in addition to SafeGuard PortProtector.

You can enter a different license key using the **Update License** button in the **Licensing** tab in the *Administration Settings* window, as shown below.

Remember that a new license overwrites the existing license. It is not appended to your current license. For example: if your current license expires in one year and you add a license for another year, you will still only have a one-year license.

To open the *Update License* window:

Click **Update License**. The window opens.


Update License
To obtain a license for SafeGuard PortProtector, you will be required to provide a fingerprint of your server machine, as well as the SafeGuard PortProtector Management Server version number.
Management Server version: 3.3.56052.51258
Server machine fingerprint: E248-4EA3
Please fill in your new server license key:
User Name:
Email Address:
License:
Import License
Confirm
License Properties
User Name: None
Email Address: None
Period: 30 days
Seats: 10
File shadowing support included
Media encryption support included
Update
Cancel

Note: When content inspection integration is activated, and additional line appears in the **License Properties** section: "Content Inspection Integration included".

7.8.1.1.1 Updating the license

1 Step 1: Obtain a license key

In order to obtain a license key, contact Sophos or your local reseller and provide the Server machine fingerprint as it appears in the screen.

For example, the fingerprint in the window above is:

"E248-4EA3"

Using this fingerprint, a license key will be generated for you and can only be used on this specific machine.

Note: You cannot use this key on any other machine. If you wish to migrate your Management Server to another machine, please contact your local reseller or Support at mailto:support@sophos.com.

2 Step 2: Enter license key

Follow the steps:

1 In the **User Name** field, enter your user name as it appears in the license key sent to you.

2 In the **Email field**, enter your email address as it appears in the license key sent to you.

3 In the **Key** field, enter the license key received.

4 Click **Confirm**. The **License Properties** are displayed, showing your updated license information, such as the allowed number of seats and the validity period of this license. In some cases, a warning message will appear after you click **Confirm**. This indicates an invalid or an expired license key.

5 Review the licensing information to ensure its correctness.

6 Click **Update** to update the license.

Note: Once you have updated the license, the previous license is completely removed. Therefore, use caution when entering licensing details.

7.8.1.2 License Usage

This field shows the number of Clients currently being served by the Management Server.

Once this number exceeds the number of licensed seats, you are requested to purchase a new license.

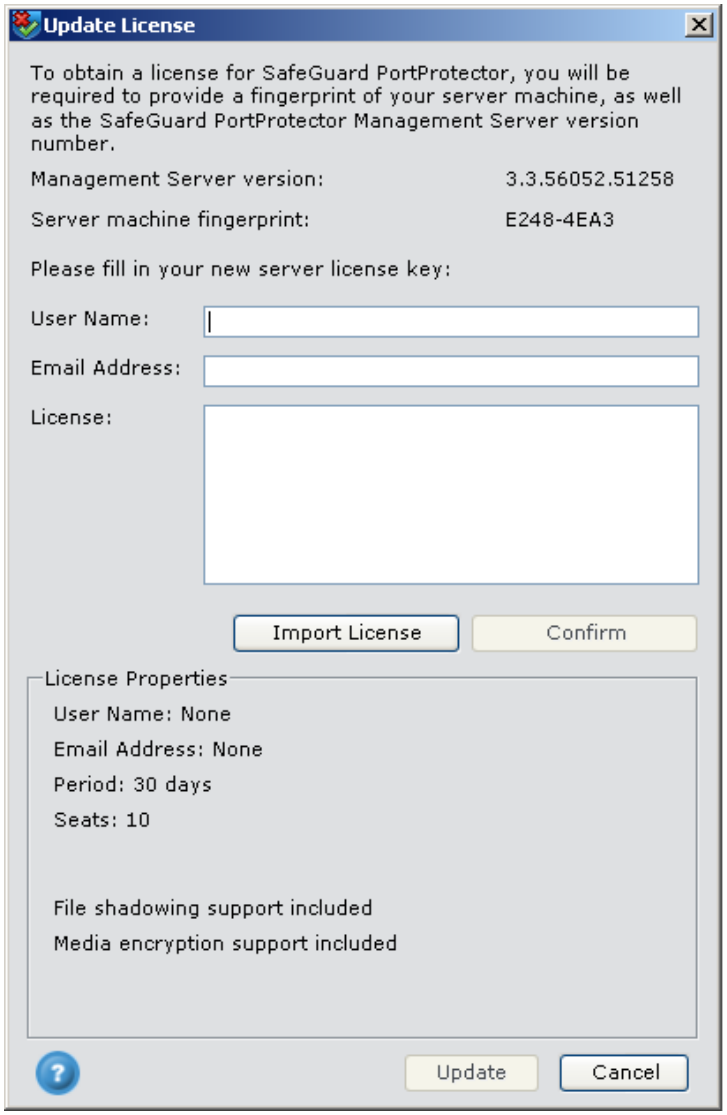
7.8.1.3 Importing an External Evaluation License

You have the option to import an external evaluation license.

To import an external evaluation license:

1 From the *Tools* menu, choose **Administration.**

2 Choose *Licensing* and click **Update Licenses.** The *Update License* dialog box is displayed.


Update License
To obtain a license for SafeGuard PortProtector, you will be required to provide a fingerprint of your server machine, as well as the SafeGuard PortProtector Management Server version number.
Management Server version: 3.3.56052.51258
Server machine fingerprint: E248-4EA3
Please fill in your new server license key:
User Name:
Email Address:
License:
Import License
Confirm
License Properties
User Name: None
Email Address: None
Period: 30 days
Seats: 10
File shadowing support included
Media encryption support included
Update
Cancel

3 Click Import License.

4 Choose the license file (.lic) in *Import license from a file.*

8 End-User Experience

About This Chapter

SafeGuard PortProtector Client should be installed on the computers of your organization in order to protect against unauthorized usage of their ports. No setup or configuration of the Client is required, and little operation exists except when encryption or decryption of storage devices is required.

You may refer to SafeGuard Policy Enforcement – SafeGuard PortProtector Client in Chapter 1, Introducing SafeGuard PortProtector for more information.

Two indications may appear on a computer that is protected by SafeGuard PortProtector according to how the administrator configured the policy, as described in *Step 15: Define Options* in *Chapter 3, Defining Policies: messages and tray icons*.

Note: When Client Visibility on Endpoints is set to Stealth Mode (see Defining client Visibility on Endpoint in *Chapter 3, Defining Policies*), messages and tray icon are hidden.

This chapter describes the user experience of being protected by SafeGuard PortProtector Client. It contains the following sections:

- ***SafeGuard PortProtector Client Messages*** describes the messages that appear in a bubble during SafeGuard PortProtector policy enforcement.
- ***SafeGuard PortProtector Client Tray Icon*** describes the tray icon states that represent the SafeGuard PortProtector Client's behavior.
- ***SafeGuard PortProtector Client Options*** describes additional options available in the Client, such as temporarily suspending protection.
- ***Panic Mode*** explains how do identify that a Client's policy has been corrupted by tampering and what to do in order to remedy this.
- ***Encryption and Decryption of Removable Storage Devices*** explains how to encrypt removable storage devices when the policy enforces encryption, and how to decrypt encrypted devices in order to use them on non-organizational computers, if the policy so permits.
- ***CD/DVD Encryption*** explains how to create encrypted volumes which you can copy to CD/DVD's and external hard disks or use as containers to store encrypted data on your hard disk.

8.1 SafeGuard PortProtector Client Messages

SafeGuard PortProtector messages begin appearing immediately after installation, according to the Options Settings defined for the policy applied to the computer/user. Whenever a message appears, you can click to close it, otherwise it disappears by itself after a few moments. Messages display the port name or the device model. They also display the texts that appear in *Step 12: Define End User Messages* in *Chapter 3, Defining Policies*, which is also where you can modify them to suit your organization.

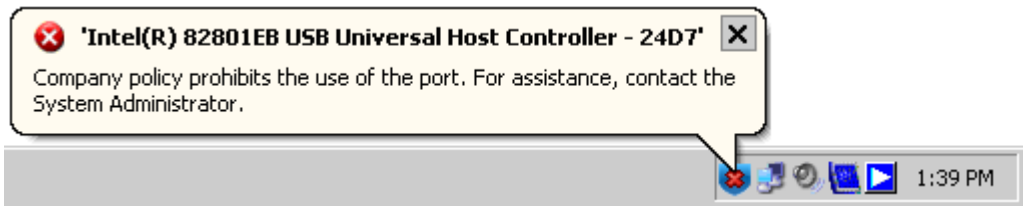
Note: The unique identifiers of distinct devices are not displayed.

Messages appear in the following cases (a description of each case follows):

- Blocked Port
- Blocked Device
- Blocked Storage Device
- Read-Only Storage Device
- Blocked File
- File Transfer Warning
- Blocked WiFi Connection
- Blocked Hardware Key Logger
- Policy Updated
- Unencrypted device connected, encrypt device (window)

8.1.1 Blocked Port

A message is displayed when a computer tries to initialize a port that has been defined as blocked. For built-in ports, this message is displayed when the endpoint computer reboots and tries to initialize the port. It is also displayed when an adapter for this port is being connected to the endpoint.


'Intel(R) 82801EB USB Universal Host Controller - 24D7'
Company policy prohibits the use of the port. For assistance, contact the System Administrator.
1:39 PM

8.1.2 Blocked Device

A message is displayed when an attempt to connect a device through one of the restricted ports is made for an unapproved device, meaning neither the device's type, model or this distinct device is approved.

'Microsoft USB Wheel Mouse Optical'
Company policy prohibits the use of the device. For assistance, contact the System Administrator.
5:17 PM

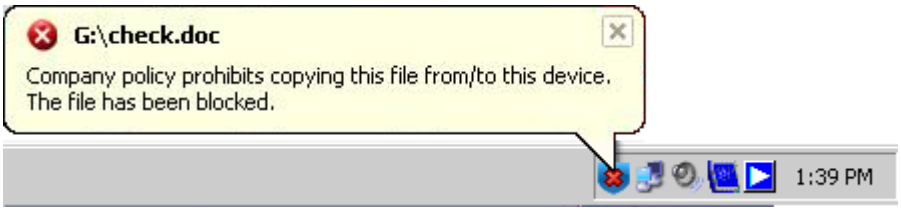
8.1.3 Blocked Storage Device

A message is displayed when a storage device whose type, model or distinct device is not approved tries to connect.

'SONY DVD RW DRU-710A'
Company policy prohibits the use of the storage device. For assistance, contact the System Administrator.
1:39 PM

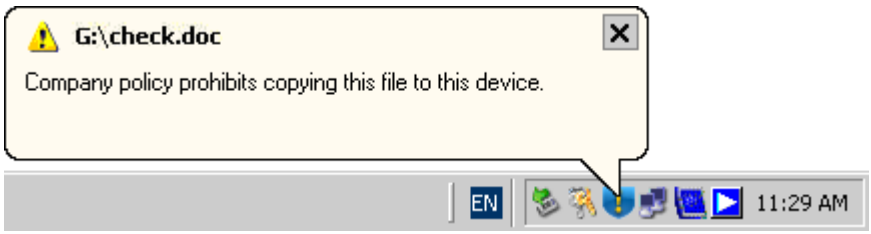
8.1.4 Blocked File

A message is displayed when the transfer of a file is blocked as a result of File Control settings.



8.1.5 File Transfer Warning

A message is displayed when a file with sensitive content (a file that has undergone Content Inspection) is written to a storage device.



8.1.6 Read-Only Storage Device

A message is displayed when a storage device that was set to have Read-Only access tries to connect. This message indicates that you can read from this storage device, but not write to it.

USB 2.0 Flash Disk USB Device
According to company policy, removable storage may only be used in read-only mode. Please contact your system administrator for further details.
EN
11:29 AM

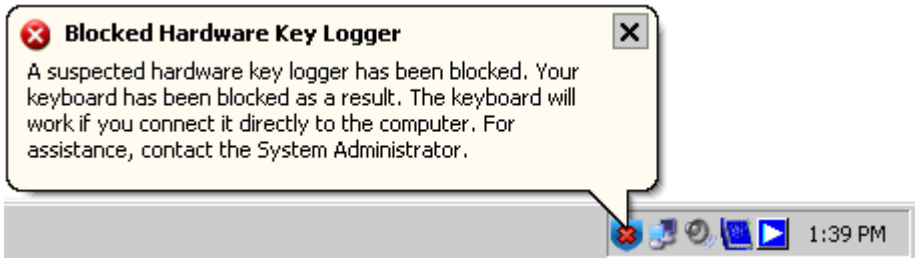
8.1.7 Blocked WiFi Connection

A message is displayed when the WiFi connection is blocked and an attempt is made to connect the host to a WiFi network. This would mean that the WiFi port was restricted and the link does not match any of the links in the white list.

My WiFi Link
The WiFi link you are trying to set up is not approved. Please contact your system administrator for further details.
1:39 PM

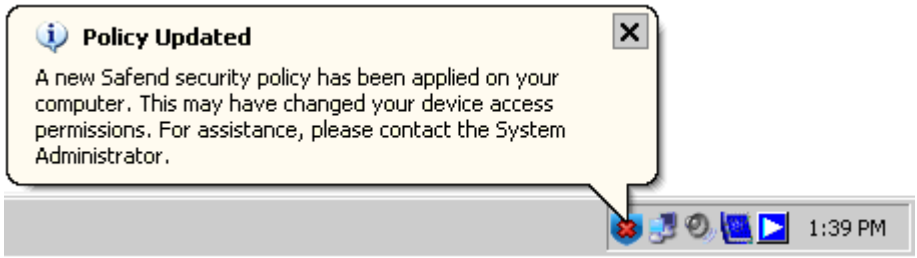
8.1.8 Blocked Hardware Key Logger

A message is displayed when a suspected USB Hardware Key Logger is connected. This disables the use of the keyboard until the Key Logger is removed.


Blocked Hardware Key Logger
A suspected hardware key logger has been blocked. Your keyboard has been blocked as a result. The keyboard will work if you connect it directly to the computer. For assistance, contact the System Administrator.
1:39 PM

8.1.9 Policy Updated

A message is displayed when a new policy is applied to the computer/user. The following describes how SafeGuard PortProtector behaves in cases where the new policy blocks a port/device/network that was previously allowed, and vice versa.


Policy Updated
A new Safend security policy has been applied on your computer. This may have changed your device access permissions. For assistance, please contact the System Administrator.
1:39 PM

8.1.10 Unencrypted Device Connected, Encrypt Device

A window opens whenever a non-encrypted device is connected and the policy mandates encryption. Through this window the device can be encrypted, as explained in *Encryption and Decryption of Removable Storage Devices*.

Close
SafeGuard® PortProtector
SOPHOS
A device is trying to connect to your computer:
Port: Universal Serial Bus
Type: Disk On Keys
Name: Disk drive / Kingston DataTraveler 2.0 USB Devic
Company policy requires encrypting this device. To start using this device you must format it.
Encrypt
Close

8.2 Allowed to Blocked

When a policy change determines that a connected device is now blocked, SafeGuard PortProtector Client will call upon the operating system and request that the device be disconnected. Occasionally, if the device is currently in use, the operating system may fail to do so. Refer to *Defining Disconnection of Active Devices* in *Chapter 3, Defining Policies* to learn how SafeGuard PortProtector Client behaves in this case.

8.3 Blocked to Allowed

When a policy change determines that a blocked device is now allowed, the (Green Checkmark) icon appears. The SafeGuard PortProtector Client will call upon the operating system and request that the device be connected. On endpoints running Windows 2000, the operating system may occasionally fail to do so and the system must be rebooted. A SafeGuard PortProtector message is displayed asking you to do so in order to connect that device.

8.4 SafeGuard PortProtector Client Tray Icon

A tray icon appears on any computer that is protected by SafeGuard PortProtector. It may appear continuously or temporarily according to how the administrator set the policy, as described in *Defining Client Visibility on Endpoints* in *Chapter 3, Defining Policies.*

Note: When Client Visibility on Endpoints is set to Stealth Mode), the tray icon is invisible.

You can hover over the tray icon to view the same information that appeared in the message. Also, on approval of a device no message is shown, and the device properties appear here. Examples are shown below:

- This is the basic SafeGuard PortProtector Client tray icon. The administrator can specify that the SafeGuard PortProtector icon is always shown in the tray, even while SafeGuard PortProtector is idle, indicating that this computer is protected by SafeGuard PortProtector.
- A port or a connected device that was blocked has becomes permitted.
- Encrypted device connected.
- Restricted to Read-Only.
- An attempt is made to use a port or device that is blocked.
- Client Protection Suspended.
- End-user entry required for removable storage device.
- Access Secure Data.

With the exception of the first icon (basic SafeGuard PortProtector Client icon) the icons appear for a few moments and then revert to the first icon.

8.4.1 Client Visibility Modes

By default, the SafeGuard icon always appears in the tray of a protected computer. This enables administrators to see at a glance that a computer is protected by SafeGuard PortProtector.

Some administrators may prefer to minimize the visibility of SafeGuard PortProtector Client on endpoints. Three visibility modes are available:

- **Full Visibility** – Always show SafeGuard PortProtector tray icon and event messages. This is the default mode.
- **Partial Visibility** – Hide SafeGuard PortProtector tray icon when idle but show event messages. In this mode the icon appear briefly when a device is connected and disappears afterwards.
- **Stealth Mode** – Hide SafeGuard PortProtector tray icon and don't show event messages In this mode, the end-user will never see the icon, and will also never receive messages on blocked devices/ports.

Note: When using encryption in your organization, the Stealth Mode should not be used so as to displays the necessary message when an unencrypted device is connected.

These options are configured in Defining Client Visibility on Endpoints in Chapter 3, Defining Policies.

8.5 SafeGuard PortProtector Client Options

In addition to protecting and monitoring host computers on an ongoing basis, SafeGuard PortProtector Client allows the end-user to perform additional actions on the host computer:

- ***Updating the Client's Policy*** instructs the Client to update the policy that protects it after the policy has been changed.
- ***Suspending SafeGuard Protection on a Client*** temporarily suspends SafeGuard protection on the host computer.
- ***Showing and Hiding File Messages*** enables end-users to hide file messages if they disrupt their work and to show them again.
- ***Creating a Virtual Encrypted Volume*** enables end-users to create encrypted containers which can be copied to CD/DVD and to external hard disks.
- ***Administrative Tasks*** enables the administrator to perform tasks such as protection suspension and keyboard reset when a Key Logger is suspected and blocked.

These actions are performed from the *SafeGuard PortProtector* Client window.

To open the SafeGuard PortProtector Client window:

1 Double-click the SafeGuard PortProtector tray icon

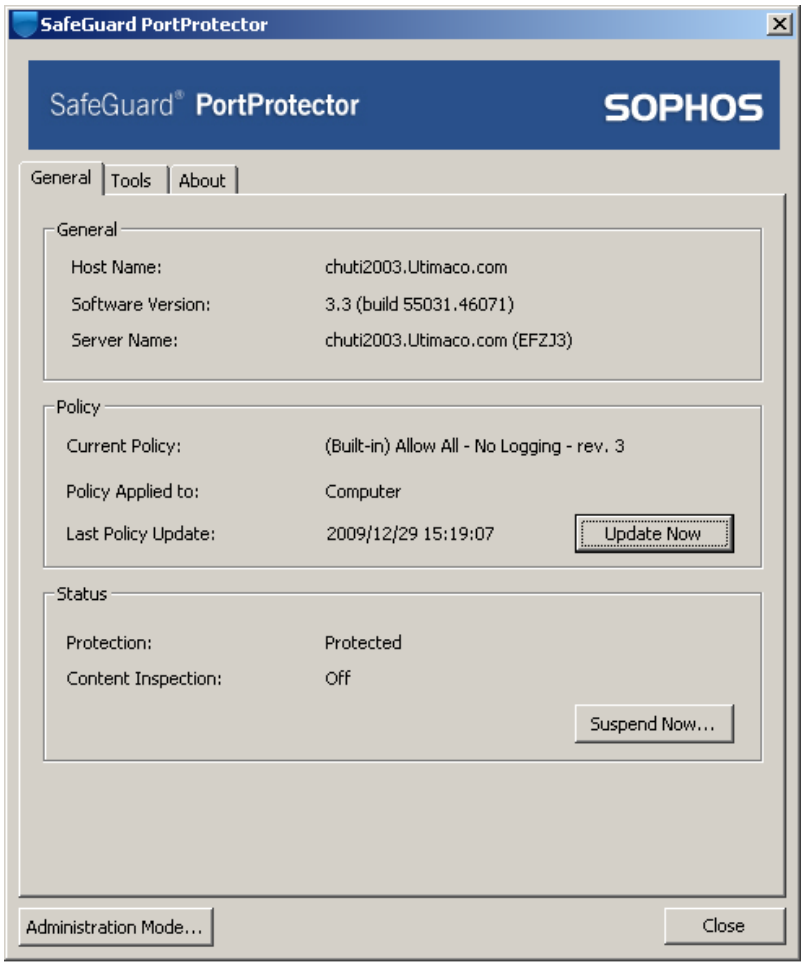
OR

Right-click the SafeGuard PortProtector tray icon and select Options

OR

From the Windows *Control Panel*, double-click the SafeGuard PortProtector icon (when the SafeGuard PortProtector tray icon is invisible only this option can be used).

2 The SafeGuard PortProtector Client window opens:



This window includes 3 tabs:

- ***General***: provides general information (host name, software version and Server name). It also displays policy information (current policy name, whether the policy is applied to the computer or its current user, and date and time of the last policy update). Thirdly, it displays Protection Status Information notifying you whether the computer is currently protected or whether protection is suspended and Content Inspection Status, showing whether content inspection is On or Off.
- ***Tools***: provides device encryption information and the ability to hide file messages on the desktop. You may refer to the *Creating and Using an Encrypted Volume* section for more information.

- ***About***: provides general SafeGuard PortProtector Client information.

The window also contains several buttons which are discussed below.

8.5.1 Updating the Client's Policy

A SafeGuard PortProtector Client's policy is updated by a process in which the Client checks the Management Server, GPO service or the registry file (depending on the policy distribution method you selected) at predefined intervals and updates the policy if it has changed. *Updating a Policy on a Client* in *Chapter 6, Managing Clients* discusses how to notify SafeGuard PortProtector Clients to refresh their policy at the earliest opportunity, through SafeGuard PortProtector Management Console. For a single, specific Client this can also be done from the host computer.

To update a policy from its host computer:

From the *General* tab of the *SafeGuard PortProtector Client* window, click **Update Now**. When an updated policy is found, a Policy Updated message appears.

8.5.2 Suspending SafeGuard Protection on a Client

As explained in *Chapter 6, Managing Clients*, if you want to temporarily suspend SafeGuard Protection on a Client without having to uninstall it, you can do so in the Management Console by generating a suspension password which you give to the user and which the user in turn enters in order to lift protection. Using this option you can suspend protection for up to a week. The next section explains what needs to be done on the Client side.

In addition, the system administrator himself/herself can suspend protection ad hoc, for a short while (no longer than one day). Both options are explained below.

8.5.2.1 Protection Suspension by the User

To suspend SafeGuard Protection, the user should do the following:

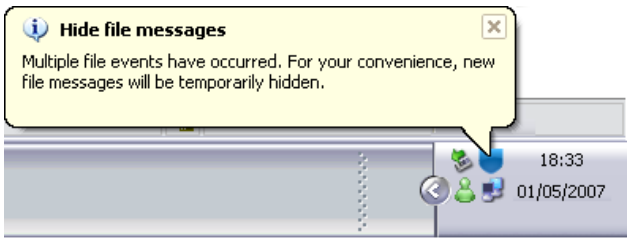
1 From the *General* tab of the *SafeGuard PortProtector Client* window, click **Suspend Now**. The *Suspend Protection* window opens.

Suspend Protection
In order to temporarily suspend the protection of the SafeGuard PortProtector, contact your administrator and ask for a password.
Host Name:
SRV-W2003.ps.utimaco.de
Enter Password:
OK
Cancel

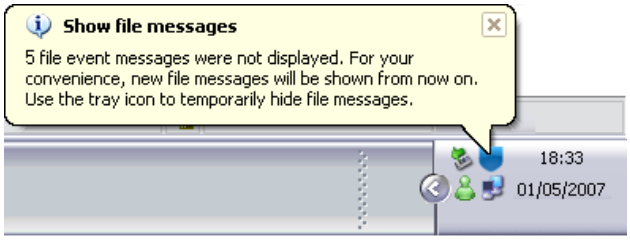
2 Enter the Suspend Password provided by the system administrator and click **OK**. A message is displayed showing the period for suspension. SafeGuard Protection is suspended on the host for the period predefined by the system administrator when generating the suspension password. At the end of this period protection is automatically resumed.

8.5.3 Showing and Hiding File Messages

As explained earlier in this chapter, file messages are displayed whenever a file transfer is blocked or a file with sensitive content is transferred to a storage device. In some cases, messages may appear too frequently as to become disruptive to the end-user's ongoing work. When SafeGuard PortProtector Client detects this (according to its hardcoded definitions), it stops displaying file messages, and displays the following message:


Hide file messages
Multiple file events have occurred. For your convenience, new file messages will be temporarily hidden.
18:33
01/05/2007

When SafeGuard PortProtector Client detects that the rate of file messages no longer causes disruption (according to its hardcoded definitions), it displays the following message:


Show file messages
5 file event messages were not displayed. For your convenience, new file messages will be shown from now on. Use the tray icon to temporarily hide file messages.
18:33
01/05/2007

Additionally, if the hardcoded threshold is unsuitable, the end-user may hide or show file messages whenever he/she wishes.

To hide file messages manually:

In the *Tools* tab of the *SafeGuard PortProtector Client* window, click **Hide File Messages**

OR

Right-click the SafeGuard PortProtector Client tray icon and select **Hide File Messages**

From this moment file messages are not shown until the end-user manually selects to show them again.

To show file messages manually:

In the *Tools* tab of the *SafeGuard PortProtector Client* window, click **Show File Messages**

OR

Right-click the SafeGuard PortProtector Client tray icon and select **Show File Messages**

From this moment file messages are shown.

8.5.4 Creating a Virtual Encrypted Volume

This option enables end-users to create encrypted containers which can be copied to CD/DVD and to external hard disks. For detailed information, please refer to *CD/DVD Encryption*.

8.5.5 Administrative Tasks

Some administrative options are available on the endpoint. These allow the administrator to perform restricted functions by using the Client Administration Password which you defined in the Policies World.

To access Administration Mode:

1 From the bottom of the *General* tab of the *SafeGuard PortProtector Client* window, click **Administration Mode**. The *Administrator Password* window opens.

2 Enter the Client Administration Password and click **OK**.

3 The window now offers two administrative functions (described below):

- Administrator Suspend
- Reset Keyboards

4 After you perform the required functions, click **Close** to close the *SafeGuard PortProtector Client* window.

5 Next time you access this window it does not offer administrative functions, until the administrator types the Client Administration Password.

Note: Always remember to close the *SafeGuard PortProtector Client* window after performing administrative tasks. Not closing the window will allow unauthorized users to perform administrative functions. Once you close the window, you will need to re-enter you administrative password in order to perform administrative functions.

8.5.5.1 Protection Suspension by the System Administrator

If you (the administrator) need to suspend SafeGuard Protection on a Client, you can do so with the Client Administration Password.

To suspend the Client:

1 Enter Administration Mode (as described above).

2 In the Protection Status section of the *SafeGuard PortProtector Client* window (the bottom section), click **Administrator Suspend**. Protection is suspended.

3 Click **Resume Now** in the Protection Status section to resume protection.

4 Close the SafeGuard PortProtector Client window.

Note: If you forget to resume protection, it will be resumed automatically 24 hours after suspension.

Note: Always remember to close the *SafeGuard PortProtector Client* window after performing administrative tasks. Not closing the window will allow unauthorized users to perform administrative functions. Once you close the window, you will need to re-enter you administrative password in order to perform administrative functions.

8.5.5.2 Reset Keyboards (approve keyboard hubs)

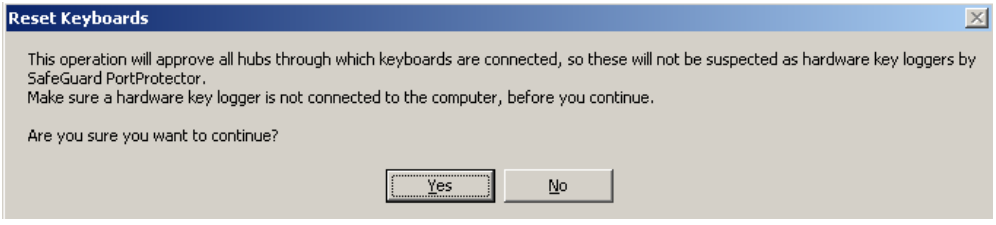
Step 5: Define Device Control in *Chapter 3, Defining Policies*, discusses how a policy can protect computers against hardware key loggers. It enables you to block a keyboard when SafeGuard PortProtector suspects that a hardware key logger is connected. In some cases when a keyboard is connected through a hub (or more than one), SafeGuard PortProtector may wrongly suspect the hub of being a key logger, and block the keyboard. Performing a "keyboard reset" as described below approves all the hubs through which the keyboard is connected at the time the reset is performed.

Note: Before resetting the keyboard you must verify that a hardware key logger is not connected, otherwise it will be approved.

To reset keyboards:

1 Enter Administration Mode (as described above).

2 In the Protection Status section of the *SafeGuard PortProtector Client* window (the bottom section), click **Reset Keyboards**. The *Reset Keyboards* window opens.


Reset Keyboards
This operation will approve all hubs through which keyboards are connected, so these will not be suspected as hardware key loggers by SafeGuard PortProtector.
Make sure a hardware key logger is not connected to the computer, before you continue.
Are you sure you want to continue?
Yes
No

3 Make sure that a hardware key logger is not connected between the keyboard and the computer.

4 In the *Reset Keyboards* window, click **OK**. All the hubs through which the keyboard is connected are now approved, and the keyboard will resume working.

Note: Always remember to close the *SafeGuard PortProtector Client* window after performing administrative tasks. Not closing the window will allow unauthorized users to perform administrative functions. Once you close the window, you will need to re-enter you administrative password in order to perform administrative functions.

8.6 Panic Mode

When a Client is tampered with, it goes into Panic mode and blocks all ports. When this happens, the *SafeGuard PortProtector Client* window displays the following message in the *Protection Status* section: "Panic (machine policy corrupted) ". An Invalid Policy log event may be issued if some parts of the policy are still intact, but if it is totally corrupted a log cannot be sent.

To overcome Panic mode, simply apply a valid policy to the Client.

8.7 Encryption and Decryption of Removable Storage Devices

SafeGuard PortProtector enables the end-user to encrypt removable storage devices and External Hard Disks. In addition to ensuring that loss or theft of the encrypted device causes no damage to the organization, this prevents leakage of information by users. As a rule, when a storage device is encrypted, it can be used only within the organizational environment, and explicit authorization is required in order to access it on non-organizational computers.

In some cases, the endpoint policy can dictate that such a storage device be encrypted, in which case encryption is mandatory. Additionally, the end-user may choose to encrypt storage devices even when the policy does not mandate it.

When the policy requires encryption, any time a user attaches a non-encrypted device, the device is either blocked or permitted Read Only access depending on policy settings (see *Step 13: Define Media* Encryption in *Chapter 3, Defining Policies)*. At the same time, the user is given the ability to encrypt the device in order to use it. This is explained in *Encrypting a Device.*

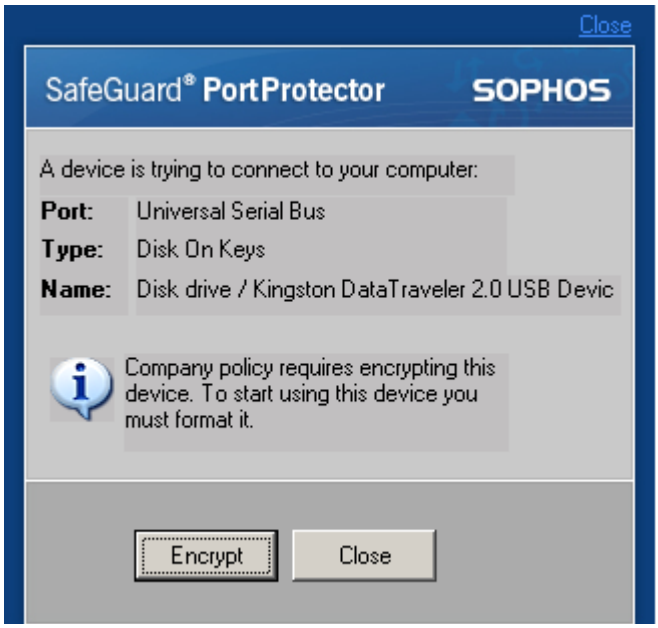
A policy can also allow authorized users access to an organizationally-encrypted device on a non-organizational computer by means of decryption.

Note: Organizationally encrypted removable storage devices and external hard disks may be used on any SafeGuard PortProtector protected organizational computers, including those whose effective policy does not require encryption.

8.7.1 Encrypting a Device

As mentioned earlier, removable storage devices and external hard disks may be encrypted, whether the endpoint policy requires it or not.

If a policy requires encryption, and a non-encrypted device is attached to the computer, the non-encrypted device is either blocked or permitted Read Only access depending on policy settings (see *Step 13: Define Media* Encryption in *Chapter 3, Defining Policies)*. In order to have full use of the device, it must be encrypted by a SafeGuard PortProtector protected computer in your organization. When a non-encrypted device is connected, a window appears informing the user of this and asking him/her to encrypt the device.


Close
SafeGuard® PortProtector
SOPHOS
A device is trying to connect to your computer:
Port: Universal Serial Bus
Type: Disk On Keys
Name: Disk drive / Kingston DataTraveler 2.0 USB Devic
Company policy requires encrypting this device. To start using this device you must format it.
Encrypt
Close

If the policy does not require encryption, the device may still be encrypted. However, in this case no end-user message appears.

To encrypt a removable storage device or an external hard disk when required by the policy:

1 In the *Unencrypted Device Connected* window that appears when you connect the device, click **Encrypt**. The following window opens for a removable storage device:

Encrypt (E:)
To start using this device as encrypted, a device format is needed.
Formatting will delete all the information currently stored on this device, unless it is backed up first.
Automatically backup and restore the data
Delete all existing data
SOPHOS
Click Next to continue.
< Back
Next >
Cancel

Note: If you have not had enough time to click the *Unencrypted Device Connected* window and it disappears, follow the instructions below for encrypting a device when no window appears.

2 Select the appropriate radio button according to whether you wish to backup and restore the data on the device or whether you wish to delete existing data (this is necessary because encrypting the device formats it).

Note: It is highly recommended to backup the information on the device before you continue with the encryption process.

3 Click **Next**.

4 If you have been assigned permission to set a password for accessing storage devices offline, then the following window is displayed. If not, then go to step **4** on the bottom of the following page.

Encrypt (E:)
A password is required to access the encrypted information.
Set Access Password
Password:
****
Confirm:
****
The password should be at least 7 characters long and should contain at least one capital letter and one digit.
SOPHOS
Click Next to continue.
< Back
Next >
Cancel

5 Enter a password that will have to be entered on computers outside your organization in order to access its content. You can always set a new password, if you forgot it.

Note: The password for offline access can also be set as described in *Setting an Offline Access Password*. It is mandatory to set a password to enable offline access in order to use the device outside of the organization.

Note: The password that you set must adhere to the organization's password rules.

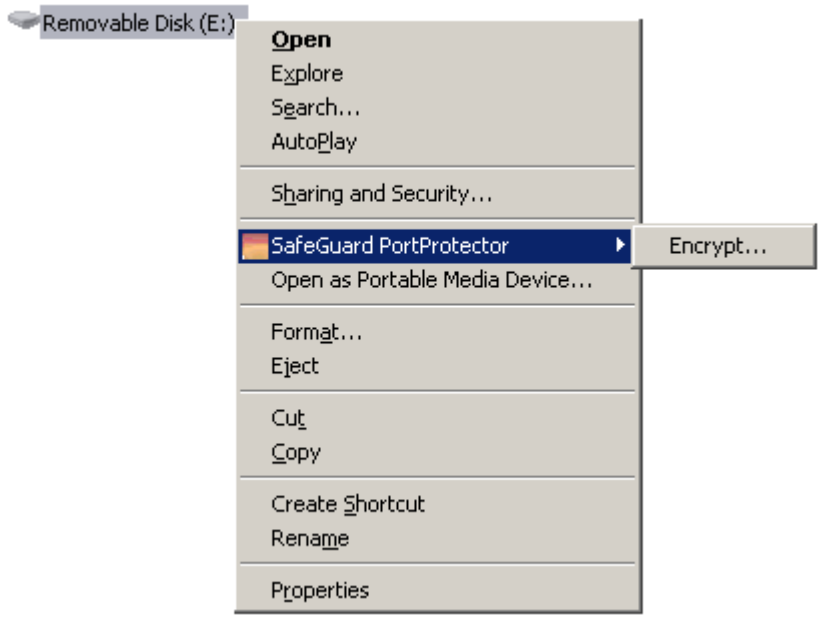
6 The encryption process (including backup and restore, if selected) begins and a progress bar appears. When the encryption process is completed, the following message appears:

Encrypt (E:)
Your device is now encrypted.
Data you store on this device will be protected in case the device is lost or stolen.
In the future, If you wish to remove the encryption from this device, or change the device password, you can start this wizard from 'My Computer'.
SOPHOS
Click Finish to exit.
< Back
Finish
Cancel

7 Click Finish. The device is now encrypted and the data stored on it is protected should the device be lost or stolen. In Windows Explorer, encrypted devices are denoted by a special icon, as in Removable Disk (E:).

To encrypt a removable storage device when no end-user window appears:

1 If the message has disappeared (it is only displayed for a few seconds), or if the policy does not mandate encryption (in which case no message appears), go to **My Computer** in Windows Explorer and right-click the device. The **SafeGuard PortProtector** option appears in the right-click menu, and the sub-menu includes the **Encrypt** option, as shown in the following figure:



2 Click **Encrypt**. The *Encrypt* window opens:

Encrypt (E:)
To start using this device as encrypted, a device format is needed.
Formatting will delete all the information currently stored on this device, unless it is backed up first.
Automatically backup and restore the data
Delete all existing data
SOPHOS
Click Next to continue.
< Back
Next >
Cancel

3 Continue from step 2 above.

8.7.2 Accessing Encrypted Devices Online

The administrator can set a policy forcing users to enter a password, within the organization, in order to access devices encrypted by anyone in their organization (even devices they have encrypted themselves).

From this point on, they are prompted to enter the device password each time the user connects the encrypted device to any protected machine in the same organization (provided the relevant policy is applied).

Close
SafeGuard® PortProtector
SOPHOS
A device is trying to connect to your computer:
Type:
Removable Media
Name:
Disk drive / CBM Flash Disk USB Device
The device is encrypted. A password is required in order to access information on this device.
Device Password:
Access the device

The device can be accessed only after the correct password has been entered.

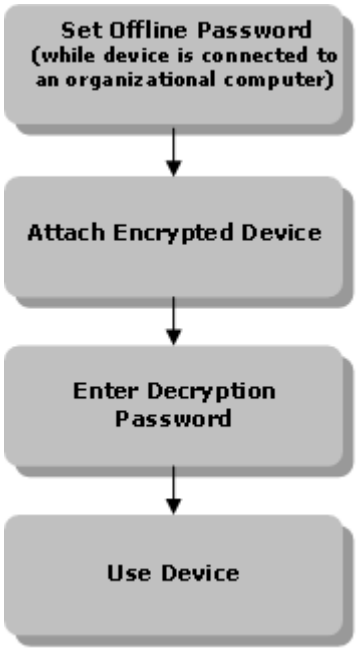
See Defining Media Encryption Settings for more information.

In the case of a user forgetting a password, the administrator can change the device password. This requires temporarily suspending Client protection. During client suspension, the user can access devices and change a device password without entering a password. So, in this way a user with the help of the administrator can set a new password for the device.

See *Suspending SafeGuard Protection on a Client* for more information.

8.7.3 Accessing Encrypted Devices when Offline

As a rule, organizationally-encrypted removable storage devices can be used only when connected to computers protected by the organization's SafeGuard PortProtector Clients. This rule notwithstanding, if the end-user's effective policy permits it (refer to *Step 13: Define Media Encryption* in *Chapter 3, Defining Policies)*, the user can have access to a removable storage device on non-company computers as well. The process of accessing encrypted devices on non-organizational computers includes the following steps:



The process is described below.

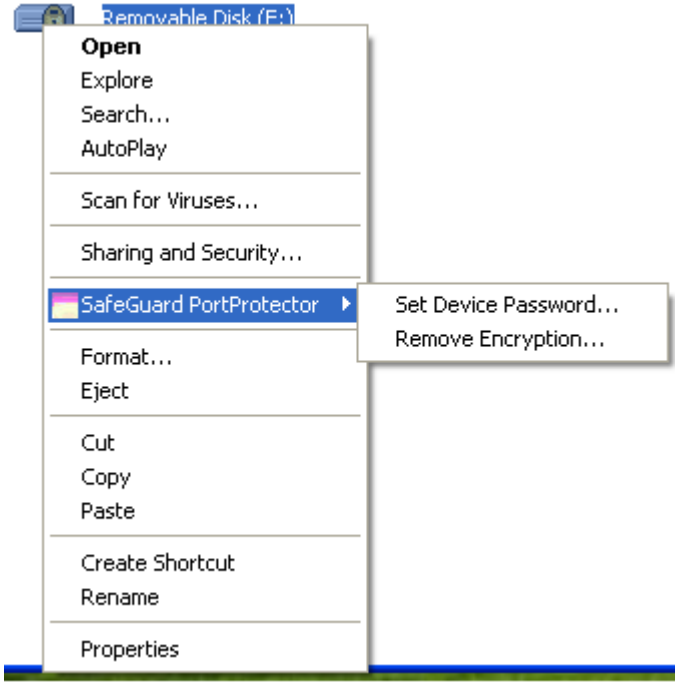
8.7.3.1 Setting an Offline Access Password

When the end-user's effective policy permits usage of encrypted devices on non-company computers, an offline access (decryption) password can be set, which will be used to access the device offline.

To set an offline access (decryption) password:

1 Connect the device you want to be able to access offline to your SafeGuard PortProtector protected computer.

2 In My Computer, right-click the device, and select the *SafeGuard PortProtector* shell extension:



3 Click **Set Device Password**. The *Set Device Password* window opens:

Set Device Password
A password is required to access the encrypted information.
Set Access Password
Password:
Confirm:
The password should be at least 7 characters long and should contain at least one capital letter and one digit.
SOPHOS
Click Next to continue.
< Back
Next >
Cancel

4 In this window, set a password, confirm it and click **Next**. The following window opens:

Set Device Password
Your new access password was successfully set.
You can always set a new password, if you forget it.
To set a new password, start this wizard from 'My Computer'.
SOPHOS
Click Finish to exit
< Back
Finish
Cancel

5 Click **Finish**. An offline access password is now set for the connected removable storage device.

Note: The password that you set must adhere to the organization's password rules.

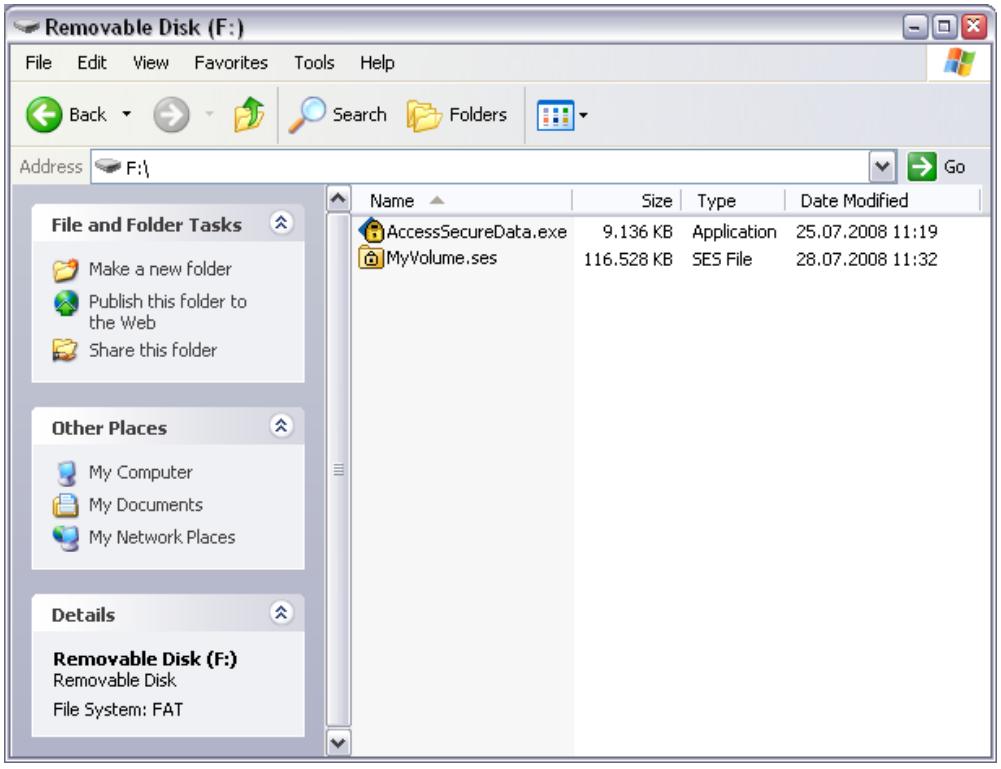
Note: If you forget it, or wish to change it, you may set a new offline access password at any time.

8.7.3.2 Offline Access to Encrypted Devices

If the endpoint policy permits it, the end-user may access organizationally-encrypted devices on non-company computers by using the offline access (decryption) password which he/she has set. Until the end-user enters the password, the only data that can be access on the device is the Access Secure Data program, which is the utility that enables entering the password.

To access an encrypted device offline:

1 Connect the encrypted device (on which an Offline Access Password has been set) to the unprotected computer. The following Windows Explorer window opens:



If you insert a removable storage device or an external hard disk and the **Device Volume Encryption** option is selected in the relevant Storage Control policy, as described in *Defining Media Encryption* Settings, then an encrypted SafeGuard PortProtector container also appears in the Windows Explorer window in addition to the Access Secure Data utility shown above. The **Device Volume Encryption** option enables offline access to storage devices by permitted users **without** requiring them to have local administration rights. Files accessed in this way can only be modified and saved using the **Save As** option, and they cannot be accessed by another application or from a command line until **Save As** is performed. This is similar behavior to an email attachment file.

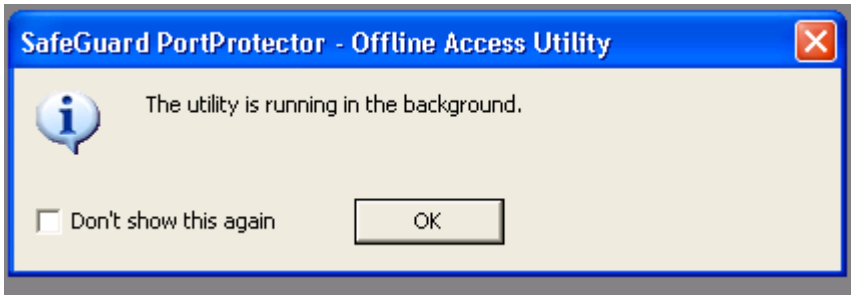
Note: Do not delete the container of the encrypted files from the removable storage device.

2 In the Windows Explorer window, double click **AccessSecureData.exe** to run it. The following window opens:

SafeGuard PortProtector - Offline Access Utility
SafeGuard® PortProtector
SOPHOS
This utility will allow you to access information on devices encrypted by SafeGuard PortProtector.
About...
Minimize

3 The utility is now running and will request the offline access password (the password which was set in *Setting an Offline Access Password*) each time an encrypted device is connected to the computer.

4 Click **Minimize** if you want to close **the window,** in which case the Access Secure Data is displayed. The following window opens:



5 Click **OK**. The utility now runs **in the** background, and will request an offline access password (the password which was set in *Setting an Offline Access Password*) each time an encrypted device is connected to the computer. Select **Exit** from the tray icon menu in order to close the utility.

Once the Access Secure Data utility is running, any time you insert an encrypted device, the Access Secure Data tray icon changes to and the following window opens from the tray:

Close
SafeGuard® PortProtector
SOPHOS
A device is trying to connect to your computer:
Type: Disk On Keys
Name: Disk drive / USB Flash Disk USB Device
The device is encrypted. A password is required in order to access information on this device.
Device Password:
Access the device

This window will remain open for a period of two minutes, during which time you may enter the device's decryption password. At the end of this period the window closes, and in order to re-open it you will need to reconnect the device. Until you enter the decryption password the encrypted device is not accessible.

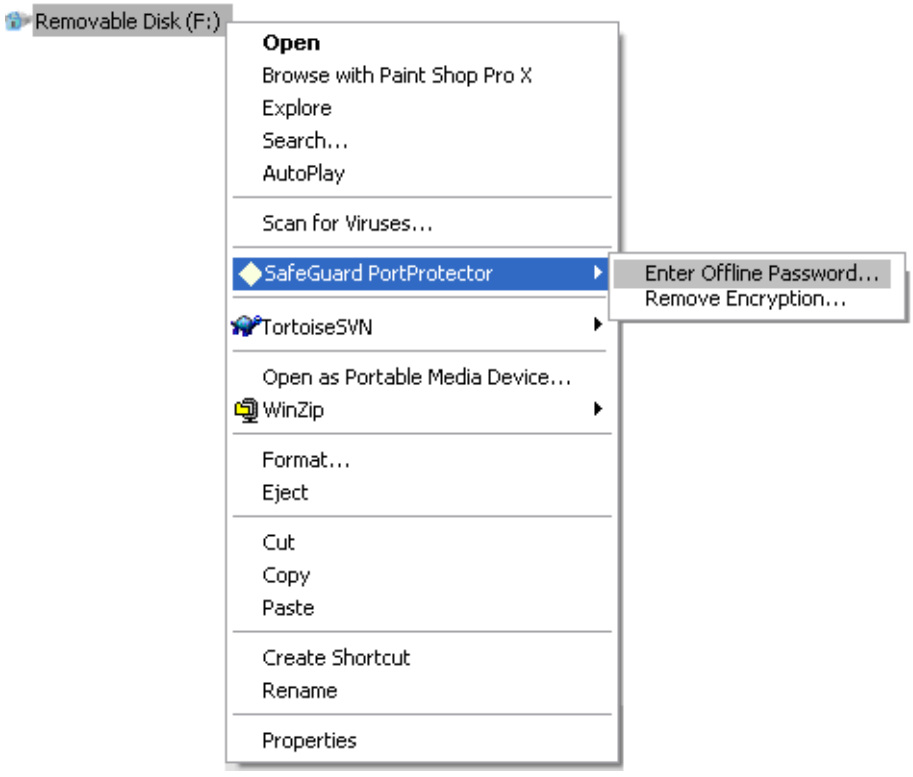
To enter an offline access password:

In the tray window, enter the Offline Access Password and click **Access the device**. The data on the device is now accessible, and the tray icon changes to **Encrypted** .

Close
SafeGuard® PortProtector
SOPHOS
A device is trying to connect to your computer:
Type: Disk On Keys
Name: Disk drive / USB Flash Disk USB Device
The device is encrypted. A password is required in order to access information on this device.
Device Password:
Access the device

Note:

If the *Offline Access Password* window disappears before you have had time to enter the password, you can set the password by right-clicking the device in My Computer, and selecting the SafeGuard PortProtector shell extension, which includes the **Enter Offline Password** option.



Note: If you disconnect the device, you will have to re-enter the decryption password next time you connect it.

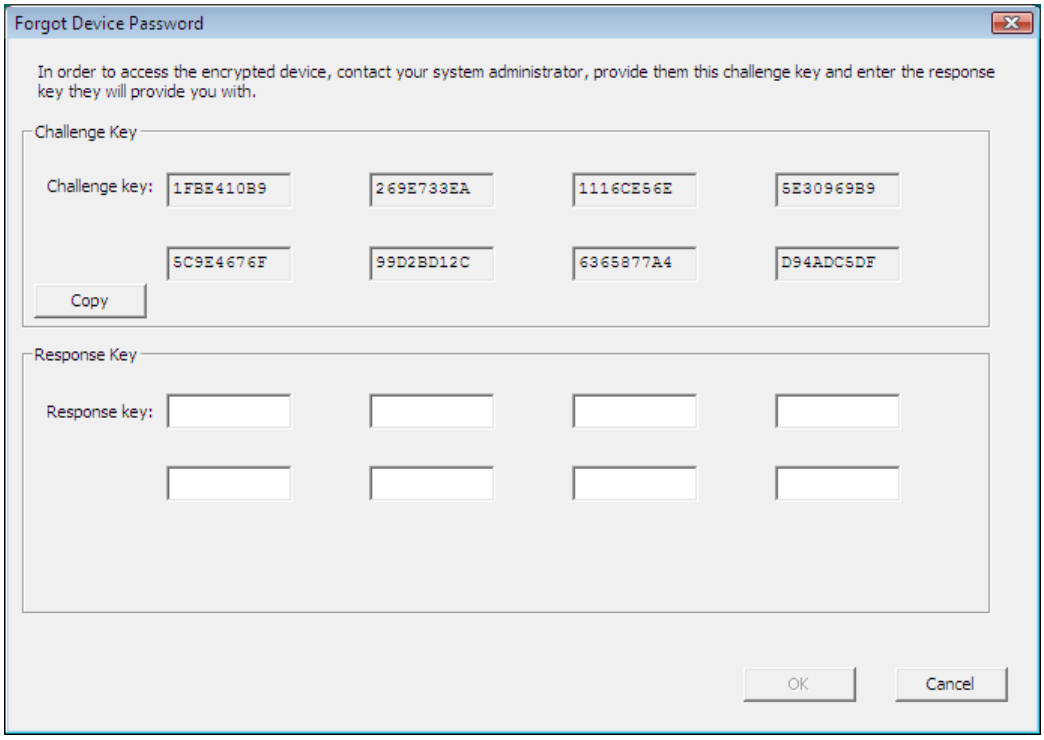
8.7.4 Granting a Device Access Key Offline

Note:

1. This procedure is only applicable to devices encrypted by the Volume Encryption method.
2. An end user requires Adminstrator privileges to perform this operation on a computer not running SafeGuard PortProtector.

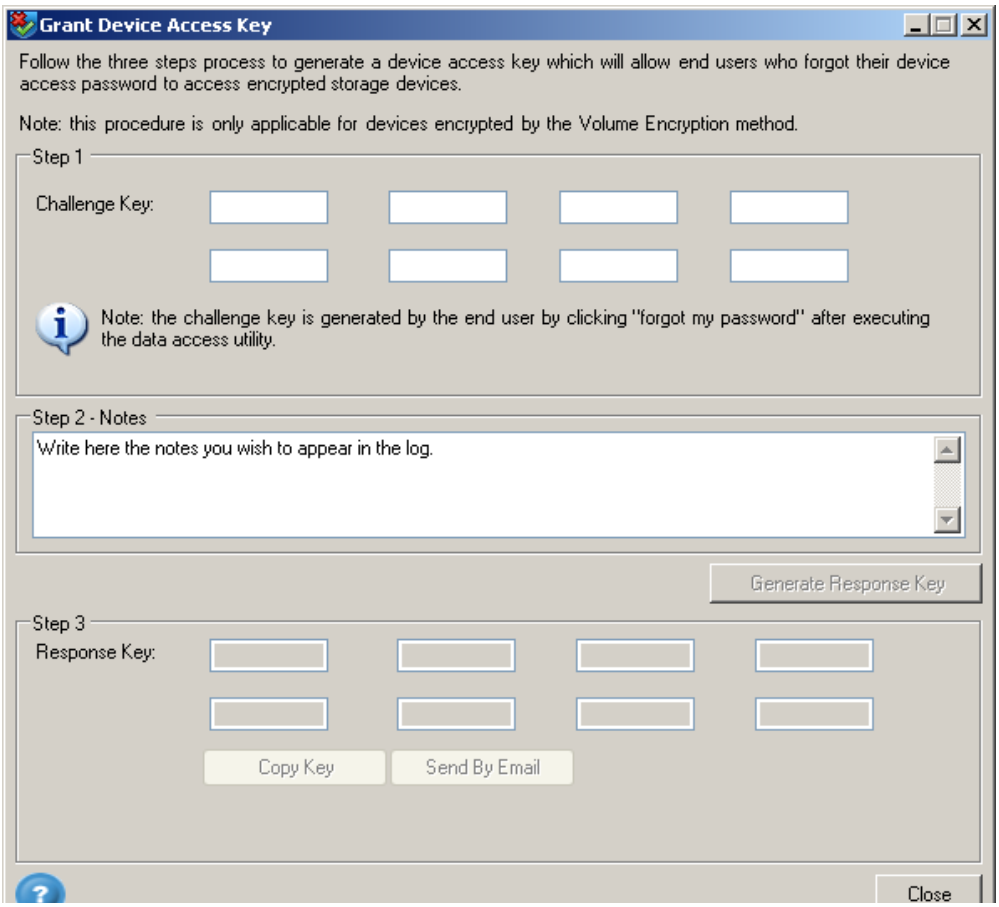
The *Grant Device Access Key* utility allows an end-user who forgot his/her password to access an encrypted removable storage device (e.g., Disk On Key) on a computer not running SafeGuard PortProtector.

The end user when accessing the data access utility clicks **Forgot my password**. The **Forgot Device Password** window is displayed.



Send the Administrator this Challenge Key (e.g., by email) and then enter the Response Key you are sent in response. Click the **OK** button. You will now have access to this device.

The administrator accesses this option from the Management Console. Click **Grant Device Access Key** from the **Tools** menu. The following window is displayed:


Grant Device Access Key
Follow the three steps process to generate a device access key which will allow end users who forgot their device access password to access encrypted storage devices.
Note: this procedure is only applicable for devices encrypted by the Volume Encryption method.
Step 1
Challenge Key:
Note: the challenge key is generated by the end user by clicking "forgot my password" after executing the data access utility.
Step 2 - Notes
Write here the notes you wish to appear in the log.
Generate Response Key
Step 3
Response Key:
Copy Key
Send By Email
Close

This contains the following steps:

Step 1: Challenge Key: These are the numbers the end user provides the administrator (e.g., by email or telephone). For each input box the characters are validated at the end of each characters sequence, if the sequence is correct the ✓ sign displayed at the right of each input box (and the input character is passed to the next characters box), if the sequence is wrong the ✗ sign is displayed and a note is displayed: "Note: incorrect challenge key was typed, please retype the challenge code."

Step 2: Notes: This is enabled after the correct challenge key is entered.Type in any note you want to appear in the log. Click the **Generate Response Key** in order to generate a response.

Step 3: Response key: These are the numbers the end user enters after receiving them from the Administrator. The same symbols will be displayed, as for the challenge key, for correct or incorrect input of characters. The **Copy Key** button enables you to copy the response key, for example to Notepad, for later use. The **Send by Email** button opens a new email message containing the response key.

Clicking the **Close** button will close the window.

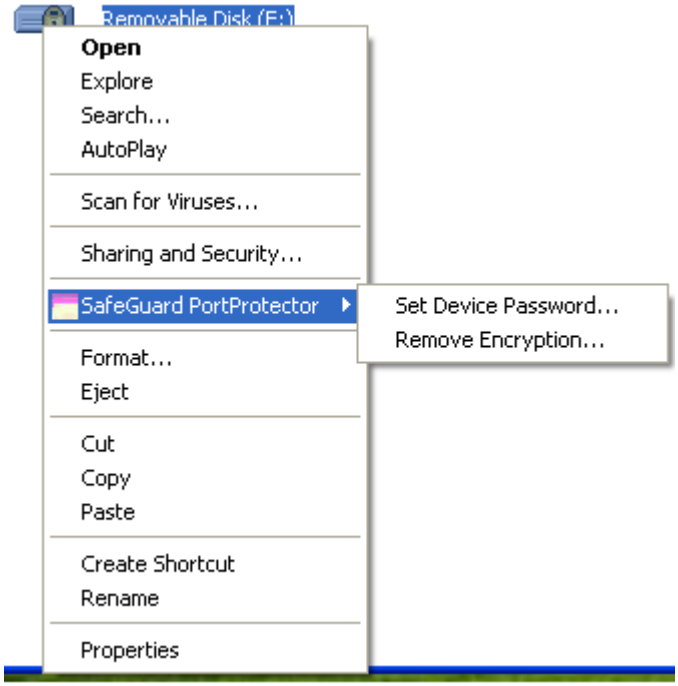
8.7.5 Removing Encryption

If you wish, you may remove encryption from encrypted devices. This is not recommended unless absolutely necessary, since the data on your device will be lost and the device will no longer be protected.

To remove encryption:

1 Connect the device.

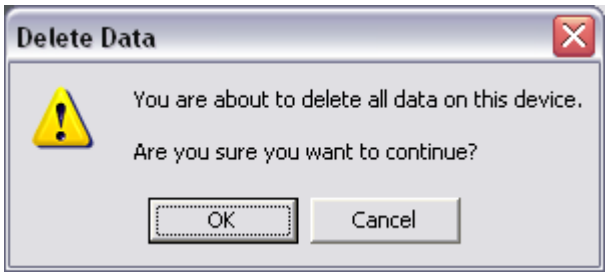
2 In My Computer, right-click the device and select the SafeGuard PortProtector shell extension



3 Select **Remove Encryption**. The following window opens:

4 Note: Removing encryption formats the device, which means all data on the device will be deleted. It is highly recommended that you backup the data before removing encryption.

5 Click **Next**. The following confirmation window opens:



6 Click **OK** to begin removal of encryption. A progress bar appears. When the process ends, the following window appears:

Remove Encryption (E:)
Encryption successfully removed from your device.
Data you store on this device will NOT be protected in case the device is lost or stolen.
It is recommended that you encrypt your device as soon as possible, to protect your data.
To encrypt the device, start this wizard from 'My Computer'.
SOPHOS
Click Finish to exit.
< Back
Finish
Cancel

7 Click **Finish** to exit the *Remove Encryption* wizard.

Attention System Administrator: End-users whose effective policy requires encryption of removable storage devices should be made aware of the instructions in *this section of the User Guide*, since their Client may launch a window that require them to encrypt removable storage devices. Users whose effective policy enables decryption and home usage of encrypted storage devices should, in addition, be provided instructions, so that they can learn how to set an offline access password and decrypt devices.

8.7.6 Tracking Offline Use of Encrypted Devices

When authorized end-users use encrypted removable storage devices on non-organizational computers, you may wish to track all the file transfers they perform from/to the device. SafeGuard PortProtector enables you to do this (refer to *Step 10: Define Logging* in *Chapter 3, Defining Policies)*.

When you activate this option, all offline file transfer information is stored on the encrypted device. Once the encrypted device is reconnected to the organizational network, all the stored logs are sent to the Management Server, and can be viewed in File Logs in the Logs World.

8.8 CD/DVD Encryption

SafeGuard PortProtector's CD/DVD Encryption provides end-users with the ability to encrypt data on CD/DVD media. Encrypted CD/DVDs are encrypted using organizational keys. This means that the folders and files they contain can be accessed on any organizational computer. It can also be accessed on an unprotected machine using the Access Utility.

8.8.1 Creating an Encrypted CD/DVD

SafeGuard PortProtector automatically launches the Create Encrypted Disc wizard which enables you to create an encrypted volume when you attempt to burn an unencrypted CD/DVD on a protected machine. It is launched in one of the following ways:

When a user who is required by policy to encrypt a CD/DVD media, inserts an empty, writeable medium to a protected machine, a window is displayed:

Click **Encrypt** to display the first page of the Create Encrypted Disc wizard, as described in step 3 below. Alternately, if you right-click on the burner drive, a menu is displayed. Select Safend Protector and then Create Encrypted CD/DVD to display the first page of the Create Encrypted Disc wizard.

8.8.2 Creating and Using an Encrypted CD/DVD

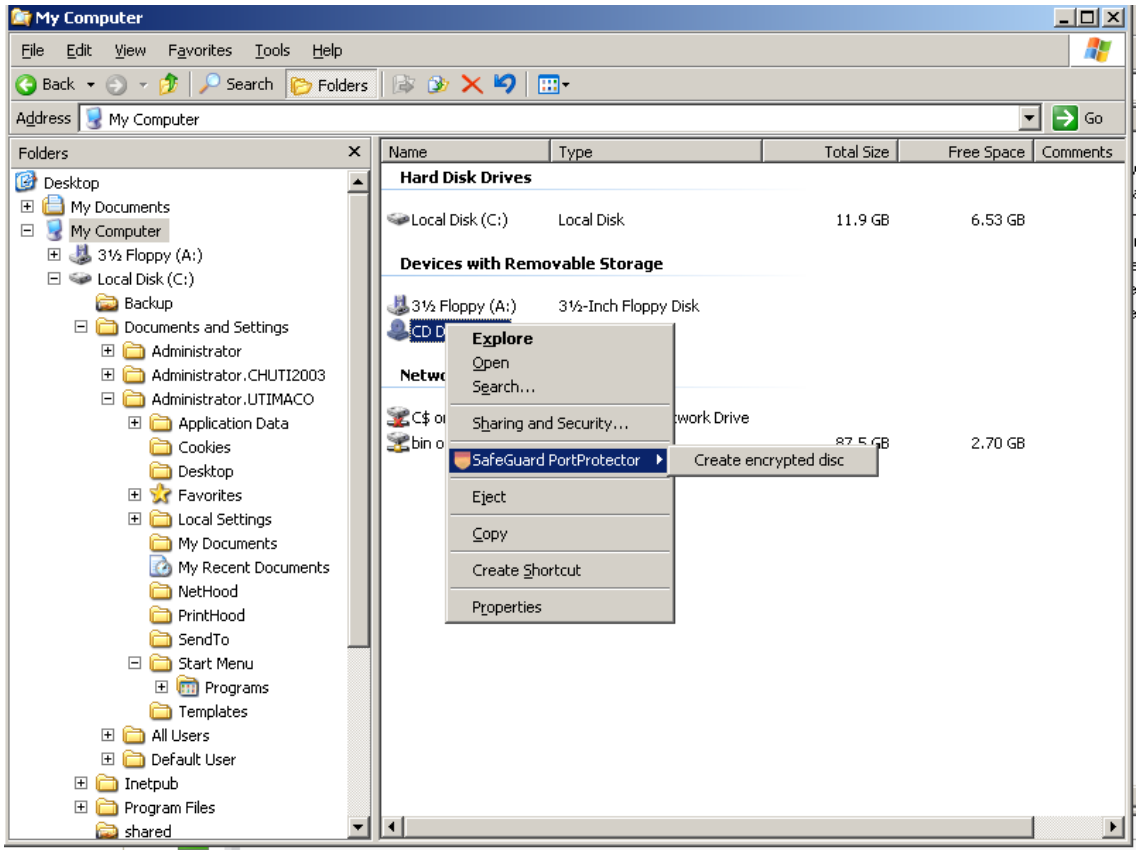
The Create Encrypted Disc wizard enables you to create an encrypted CD/DVD media.

To access the Create Encrypted Disc wizard:

You can access the Create Encrypted Disc wizard in 2 ways:

1 Right click on a CD/DVD drive.

2 Select SafeGuard PortProtector and then select **Create Encrypted CD/DVD**, as shown below.



Or else From the SafeGuard PortProtector Client window:

Double-click the SafeGuard PortProtector tray icon

OR

Right-click the SafeGuard PortProtector tray icon and select Options

OR

From the Windows Control Panel, double-click the SafeGuard PortProtector icon when the SafeGuard PortProtector tray icon is invisible only this option can be used).

The SafeGuard PortProtector Client window opens.

1 In the Safend Protector Client window, click the Tools tab. The following window opens:

2 Click the Encrypt Disc button.

3 The Create Encrypted Disc wizard is displayed.

4 To access the Create Encrypted Disc wizard:

5 This wizard will guide you through the process of creating an encrypted CD/DVD.

6 Access the Create *Encrypted Disc* wizard as described above. The following wizard is displayed.

7 Specify the *Disc Size*. Select one of the standard sizes for a CD or DVD or enter its size in the Other field. Click **Next**.

8 If you have been assigned permission to set a password for accessing storage devices outside the organization, then the following window is displayed.

Create Encrypted Disc
A password is required to access the encrypted information on other computers. You will be prompted for this password only on computers outside your organization.
Set Access Password
Password:
Confirm:
The password should be at least 7 characters long and should contain at least one capital letter and one digit.
SOPHOS
Click Next to continue.
< Back
Next >
Cancel

9 Choose a password that will be used on computers outside your organization in order to access its content. You can only set a password **before burning** the CD/DVD.

Note: The password that you set must adhere to the organization's password rules.

10 Click **Next**. The following window is displayed:

Create Encrypted Disc
Open the encrypted volume folder and add files from your computer. These files will be burned on the encrypted disc:
Open Volume...
Note: close the volume window before you continue with the burning process
Click Next to continue.
SOPHOS
< Back
Next >
Cancel

11 Click **Open Volume** and add files from your computer to the encrypted disc.

12 Click **Next**. The following window is displayed:

13 Choose the *Burner Drive* and *Burner Speed* for the CD. Click **Refresh** to change the CD or Burner. Select *Verify data after burning* if you want to check that the data is on the disc.

14 Click **Burn** to start the process. The progress will be displayed in *Burning Progress*.

15 Note:

16 In Windows 2000 the behavior is different. Contact Sophos suport for more information.

17 Click Finish to exit the wizard.

8.8.3 Offline Access to Encrypted CD/DVDs

Access to an encrypted CD/DVD will differ depending on whether or not you have administrator privileges. See the description at the end of the section *Offline Access to Volume Encrypted Devices* for more details.

9 Appendix A – Novell eDirectory Synchronization

About This Appendix

Similarly to its existing seamless integration with Active Directory, SafeGuard PortProtector supports full integration with Novell's eDirectory. With this integration the Management Server can be configured to connect to the eDirectory in order to import the organizational tree, including OUs, Groups, Users and Computers. This enables viewing of directory objects (computers/user groups) through the Management Console for policy association, log filtering and Client management purposes.

When you configure a SafeGuard PortProtector system to synchronize with eDirectory, you will typically choose to distribute policies using the Policy Server (see *Distributing SafeGuard PortProtector Policies Directly from the* in *Chapter 4, Distributing Policies*). However, if you wish to use a different distribution method, such as a third party tool using registry files, you can do so. To learn about policy distribution methods refer to *Chapter 4, Distributing Policies*.

9.1 Configuring SafeGuard PortProtector to Synchronize with Novell eDirectory

Configuring SafeGuard PortProtector to synchronize with Novell eDirectory is performed in the *Administration* window and explained below (refer to *Chapter 7, Administration* for further details about the *Administration* window).

Note: There is no need for a Novell client to be installed on the SafeGuard PortProtector Management Server machine.

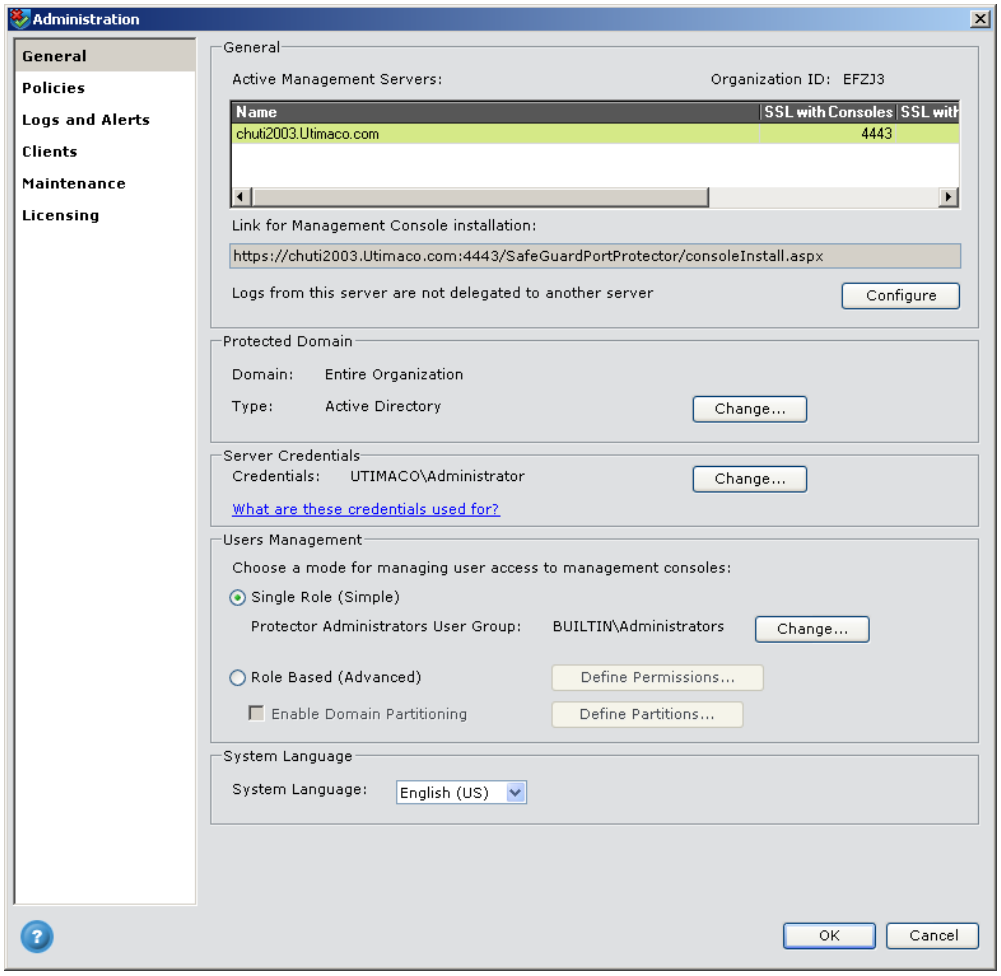
To open the *Administration* window:

From the *Tools* menu, select **Administration**

OR

In the Home World, from the *More* section, click the **Change Administration Settings** link.

The *Administration* window opens:

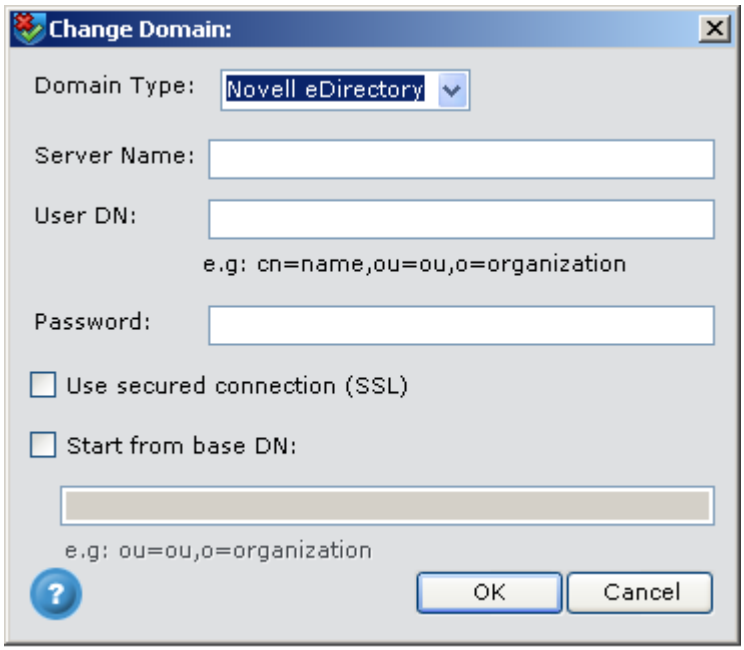


The default Directory setting is an Active Directory. To synchronize with Novell eDirectory instead, you need to change this setting.

To change Directory setting:

1 In *General* page, in the **Protected Domain** section, click **Change**. The *Change Domain* window opens:

2 In the **Domain Type** field, select **Novell eDirectory** from the drop-down menu.



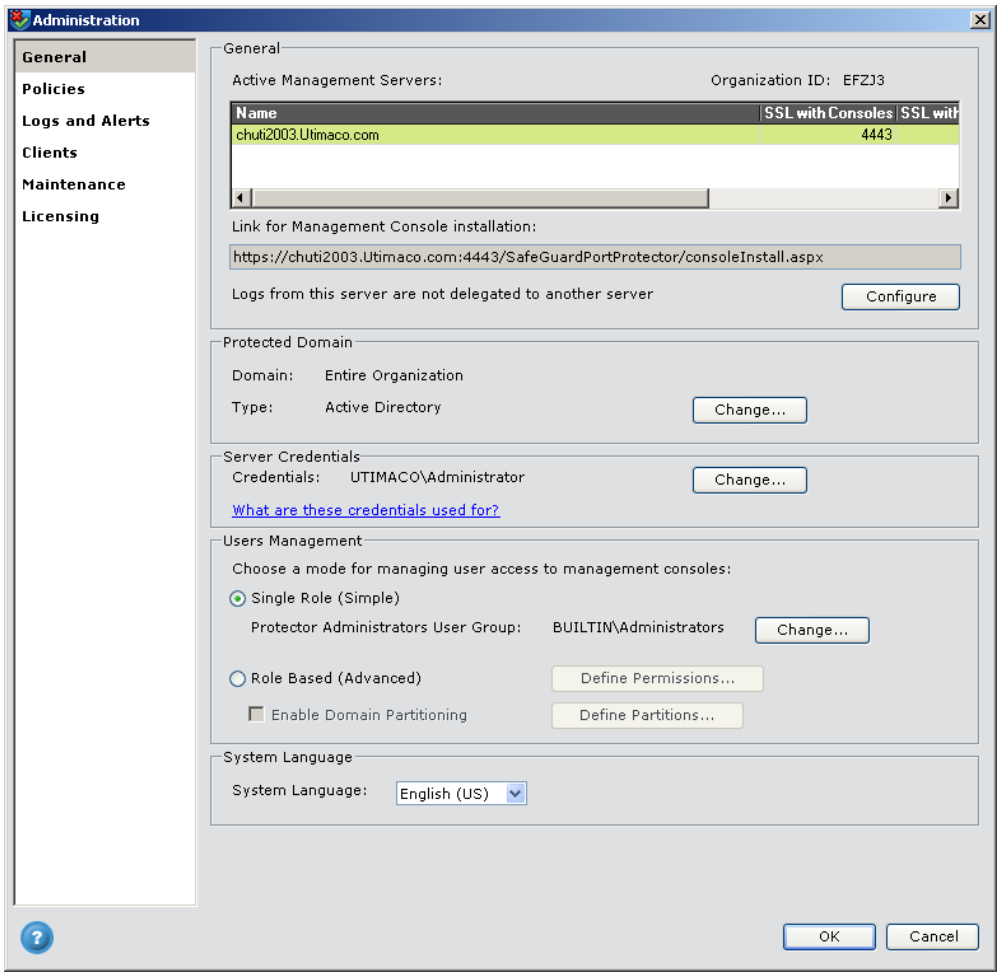
3 In the **Server Name** field, enter the Novell server name.

4 In the **User DN** field, enter the user information**.** This user should have reading privileges for all Novell objects. The format is cn=name,ou=ou,o=organization.

5 In the **Password** fields enter the user's password.

6 If you want to protect starting from a specific DN, in order to protect a specific branch or office and not the entire organization, check the **Start from Base DN** checkbox and enter the DN. If you want to apply protection to the entire organization, leave the checkbox unchecked.

7 Click **OK** to return to the *Administration* window:



8 In the *Administration* window, click **OK**.

9 SafeGuard PortProtector will now be synchronized with eDirectory. All previous tree objects are deleted.

Note: When using Novell, it is best to perform the above configuration prior to installing Clients. This way, the Client installation will contain the appropriate configuration and Clients will immediately identify themselves as Novell clients.

Note: If you previously had policies applied to deleted AD tree objects, you can still view their logs through querying logs by name.

9.2 A Few Additional Points

- When using Novell, role-based administration (explained in *Role Based (Advanced)*
- in *Chapter 7, Administration*) is possible only using local groups on the Management Server.
- SafeGuard PortProtector Client detects changes in the Novell user logged in to the endpoint using login and changes the effective endpoint policy accordingly. In-session user changes are not detected. This means that the previous user's policy remains effective until it is either updated from the *Client* window (see *Updating the Client's Policy* in *Chapter 9, End-user Experience*) or until the next update occurs according to the policy update interval.
- In logs, Novell objects appear in type-less format (for example mike.pm.acme.com)

10 Appendix B - Supported Device Types

About This Appendix

This appendix lists the device types that SafeGuard PortProtector provides for your selection when building a policy.

For **non-storage devices** you can restrict the usage of devices on USB, FireWire and PCMCIA ports. SafeGuard PortProtector provides a selection of built-in types in the *Device Control* window to enable you to define which types of devices are approved or blocked. If you require control of a device type that is not listed here, you can use the Distinct Device restriction feature described in *Approving Devices and WiFi Connections* in *Chapter 3, Defining Policies*.

For **storage devices**, SafeGuard PortAuditor is able in most cases to identify whether a device is a storage device or a non-storage device, by detecting its volume, or using its embedded class data. This ability helps categorize and organize device lists into storage devices and simple (non-storage) devices for your selection, thus enabling you to define your policy more easily. SafeGuard PortProtector provides a selection of built-in types in the *Storage Control* window to enable you to define which types of devices will be approved or blocked, as described in *Chapter 3, Defining Policies.*

The following device type lists are divided into Non-Storage Devices and Storage Devices.

10.1 Non-Storage Device Types

The following lists the non-storage built-in device types for which a policy can be defined in SafeGuard PortProtector.

Note: Device Control for non-storage devices can only be defined for USB, FireWire and PCMCIA ports.

- Human Interface Device - devices used to control the operation of computer systems. Typical examples include keyboards and pointing devices, such as: mouse, trackballs and joysticks.
- **Printing Devices** – Printers connected over USB, PCMCIA or FireWire
- Personal Data Assistants (PDA's) - These include:
- Windows Mobile / Pocket PC Devices
- Blackberry Devices
- Palm OS Devices
- **Mobile Phones** – New models of cellular phones, categorized in USB as 'Wireless USB Devices'
- **Network Adapters** - Communication devices such as: Ethernet network adapters, WiFi adapters and USB-connected ADSL and cable modems.
- **Imaging Devices** - Primarily devices such as scanners and digital still cameras.

- **Audio/Video Devices** - devices such as: microphones, telephones, volume controls, web cameras, digital camcorders, digital television tuners and digital still-image cameras that support video streaming.
- **Smart Cards** - Smart Card devices.
- **Content Security Devices** - used to provide special security features, such as strong authentication, biometric identification and software licensing.

10.2 Storage Device Types

Protection of storage devices applies to all non-blocked ports, meaning that it applies to the specified storage device no matter to which port it is connected as long as that port is not defined as blocked.

Note: Device Control for storage devices can be defined for any port type including, for example, parallel ports, USB, FireWire and PCMCIA ports.

Internally attached storage device are also controlled.

The following lists the storage built-in device types that are supported by SafeGuard PortProtector.

- **Removable storage devices** - These devices range from storage-only devices, such as disk-on-key, Memory Sticks and SD flash cards, to devices that have a unique purpose, but appear to the computer as a new storage drive, such as portable digital music players, digital cameras and PDAs.
- **External Hard Disks –** hard disk devices which are externally attached (e.g. via USB)
- **CD/DVD Drives** – both internally and externally attached
- **Floppy Drives** - both internally and externally attached
- Tape Drives - both internally and externally attached

11 Appendix C – Supported File Types

About This Appendix

The following table lists the file types and extensions supported by SafeGuard PortProtector's File Type Control, described in *Step 7: Define File Control* in *Chapter 3, Defining Policies*.

File Type	Extensions	Description
Microsoft Office	DOC	Microsoft Word Document
	DOCX	Microsoft Word Document
	DOCM	Microsoft Word Document
	DOT	Microsoft Word Template
	DOTX	Microsoft Word Template
	DOTM	Microsoft Word Template
	RTF	Rich Text Format
	PPT	Microsoft PowerPoint Presentation
	PPTX	Microsoft PowerPoint Presentation
	PPTM	Microsoft PowerPoint Presentation
	POT	Microsoft PowerPoint Template
	POTX	Microsoft PowerPoint Template
	POTM	Microsoft PowerPoint Template
	PPS	Microsoft PowerPoint Show
	PPSX	Microsoft PowerPoint Show
	PPSM	Microsoft PowerPoint Show
	PPA	Microsoft PowerPoint Add-In
	PPAM	Microsoft PowerPoint Add-In
	XLS	Microsoft Excel Workbook
	XLSX	Microsoft Excel Workbook
	XLSM	Microsoft Excel Workbook
	XLSB	Microsoft Excel Workbook
	XLT	Microsoft Excel Template
	XLTX	Microsoft Excel Template
	XLTM	Microsoft Excel Template
	XLA	Microsoft Excel Add-In
	XLAM	Microsoft Excel Add-In

File Type	Extensions	Description
	MPP	Microsoft Project Project
	MPT	Microsoft Project Template
	VSD	Microsoft Visio Drawing
	VDX	Microsoft Visio Drawing
	VSS	Microsoft Visio Stencil
	VSX	Microsoft Visio Stencil
	VST	Microsoft Visio Template
	VTX	Microsoft Visio Template
	PUB	Microsoft Publisher
	ONE	Microsoft OneNote Sections
	ADP	Microsoft Access Project
	ADE	Microsoft Access Project Extension
Published Documents	PDF	Adobe Acrobat Document
	PS	Post Script Document
	EPS	Encapsulated Post Script
Web Pages	HTML	HTML Web Page
	HTM	HTML Web Page
	MHT	Archived Web Page
	MHTML	Archived Web Page
	PHP	PHP Script
	HLP	Windows Help File
	CHM	Compiled Help File
	ASP	Active Server Page
	ASPX	ASP.NET Web Page
	ASMX	ASP.NET Webservices
	JHTML	Java HTML Web Page
	JSP	Java Server Page
Images	JPG	JPEG Image
	JPEG	JPEG Image
	GIF	GIF Image
	BMP	Bitmap Image
	DIB	Device Independent Bitmap Image
	PNG	PNG Image
	TIF	Tagged Image Format
	TIFF	Tagged Image Format
	MDI	Office Document Imaging File

File Type	Extensions	Description
	JNG	JNG Image
	MNG	MNG Image
	ICO	Windows Icon
	CUR	Windows Cursor
	WMF	Windows Metafile Image
	EMF	Enhanced Windows Metafile Image
	FH9	Macromedia Freehand 9 Graphics
	JP2	JPEG-2000 Image
	PBM	Portable Bitmap
	PGM	Portable Graymap Bitmap
	PPM	Portable Pixelmap Bitmap
	PSD	Adobe Photoshop Graphics
	CDR	CorelDRAW Vector Graphics
	SVG	Scalable Vector Graphics
Multimedia	WAV	Waveform Audio
	WMA	Windows Media Audio
	MP2	MPEG Audio
	MP3	MPEG Audio
	AIFF	Audio Interchange
	AIF	Audio Interchange
	AU	AU Audio
	RA	RealMedia Streaming Media
	MID	Musical Instrument Digital Sound
	MIDI	Musical Instrument Digital Sound
	RMI	Musical Instrument Digital Sound
	SDS	Musical Instrument Digital Sound Sample
	VOC	Creative Lab's Soundblaster Audio
	OGG	Ogg Vorbis Codec Audio
	VOX	Dialogic Audio
	FLAC	Free Loseless Codec Audio
	MPEG	MPEG Multimedia
	MPG	MPEG Multimedia
	AVI	Audio Video Interleave
	ASF	Advanced Streaming Format
	WMV	Windows Media Multimedia
	MOV	QuickTime Video Clip

File Type	Extensions	Description
	SWF	Flash Animation File
	FLI	FLIC Animation
	FLC	FLIC Animation
Text & Program Code	TXT	Text File
	CSV	Formatted Text (Comma Delimited)
	PRN	Formatted Text (Space Delimited)
	CPP	C++ Program Code
	C	C/C++ Program Code
	H	C/Java Header File
	XML	XML File
	F	FORTRAN Program Code
	T90	FORTRAN Program Code
	MAKEFILE	Compilation Control File
	MAKEFILE.IN	Compilation Control File
	PL1	PL1 Program Code
	ASM	Assembler Progeam Code
	PAS	PASCAL Program Code
	JAVA	JAVA Program Code
	M4	Meta4 Program Code
	BCPL	BCPL Program Code
	CS	Visual C#.NET Program Code
	PL	Perl Program Code
	PM	Perl Program Code Module
	PY	Python Program Code
	PDB	Visual C++/.NET Program Database
	BAS	BASIC Program Code
	VB	Visual Basic Program Code
	VBS	VBScript Script
	JS	JavaScript Source Code
Executables	EXE	Executable
	DLL	Dynamic Link Library
	PIF	Windows Program Information File
	BAT	Batch
	COM	Command
	OCX	ActiveX - Object Linking and Embedding (OLE) Control Extension

File Type	Extensions	Description
	CMD	Command
	CPL	Windows Control Panel Extension
	SCR	Windows Screen Saver
	VXD	Virtual Device Driver
	SYS	System Device Driver
	CLASS	Java Bytcode
	PYC	Python Compiler Script (Bytecode)
	LIB	Program Library Common Object File Format (COFF)
	INS	InstallShield Script
	OBJ	Object File
	O	Object File
Compressed Archives	ZIP	ZIP Compressed Archive
	ARJ	ARJ Compressed Archive
	RAR	WinRAR Compressed Archive
	GZIP	GZIP Compressed Archive
	TAR	Tape Archive
	JAR	JAR Compressed Archive
	ACE	WinAce Compressed Archive
	HQX	Macintosh BinHex 4 Compressed Archive
	LZH	LHA Compressed Archive
	LHA	LHA Compressed Archive
	AR	AIX Small Indexed Archive
	ARC	LH ARC Compressed Archive
	CAB	Cabinet Compressed Archive
	**_	Compressed Installation Files (e.g. EX_, DL_)
CD/DVD Disc Images	ISO	ISO Disc Image
	BIN	BIN Disc Image
	CIF	EasyCD Creator Disc Image
	CCD	CloneCD Disc Image
	IMG	CloneCD Disc Image
	MDF	Alcohol 120% Disc Image
	DAA	PowerISO Disc Image
	C2D	WinOnCD Disc Image
Databases	MDB	Microsoft Access Database
	ACCDB	Microsoft Access Database

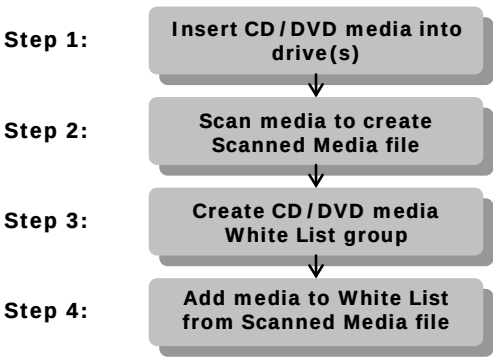
File Type	Extensions	Description
	ACCDT	Microsoft Access Database Template
	MDA	Microsoft Access Add-In
	MDW	Microsoft Access Workgroup
	MDE	Microsoft Access Compiled Database
	MYD	MySQL MyISAM Database
	MYI	MySQL MyISAM Database Index
	FRM	MySQL MyISAM Generic Dictionary
	DBF	dBase Database
	DBT	Microsoft FoxPro Database
	GDB	Borland InterBase Database
	PX	Paradox Database
Microsoft Outlook	PST	Outlook Personal Folder
	DBX	Outlook Express E-mail Folder
PGP Encryption	PGP	Pretty Good Privacy (PGP) Encrypted
	ASC	Pretty Good Privacy (PGP) Armored Encrypted
	CTX	Pretty Good Privacy (PGP) Ciphertext
Computer-Aided Design (CAD)	DWG	AutoCAD Drawing
	DXF	AutoCAD Interchange
	ASM	Pro/ENGINEER Assembly
	PRT	Pro/ENGINEER Model
Adobe FrameMaker	DOC	Adobe FrameMaker/FrameBuilder Document
	FM	Adobe FrameMaker Document
	FRM	Adobe FrameMaker Document
	BOOK	Adobe FrameMaker Book
	MIF	Adobe FrameMaker Interchange Format

12 Appendix D – CD/DVD Media Scanner

About This Appendix

In addition to controlling CD/DVD drives, SafeGuard PortProtector includes the ability to identify specific CD/DVD media, in order to authorize their use. A special scanning mechanism known as the Media Scanner computes a unique "fingerprint" identifying the data on each medium, and adds the medium's details to its output file (the Scanned Media file). The Media Scanner may be used on any computer and does not require any network connection to the Management Server. This allows you to run the utility on a stand-alone machine in order to avoid the inherent risks of viruses and Trojans which can be introduced via CDs and DVDs.

From the output file, scanned media can then be added to a CD/DVD Media White List in order to authorize their use. This means that any medium that is not white-listed is prohibited, unless it is used through a specific, white-listed CD/DVD drive (CD/DVD media and device white lists are explained in detail in *Chapter 3, Defining Policies*.) Any change made to the data on the medium following the scan will revoke its fingerprint, and in turn make it unapproved. The process of fingerprinting media and adding them to the CD/DVD Media White List is summarized in the following chart:


Step 1:
Insert CD/DVD media into drive(s)
Step 2:
Scan media to create Scanned Media file
Step 3:
Create CD/DVD media White List group
Step 4:
Add media to White List from Scanned Media file

The process of creating a CD/DVD media White List (steps 3 and 4) is explained in *Approving CD/DVD Media* in *Chapter 3, Defining Policies*.

12.1 Scanning and Fingerprinting Media

Before a CD/DVD medium can be authorized by adding it to a CD/DVD Media White List, it must be scanned in order to "fingerprint" it and add the fingerprinted medium's details to an output file (referred to below as the Scanned Media file). This is performed using the Media Scanner, provided with the installation package. The Media Scanner can be run on any computer.

Note: Audio CDs are not supported by the Media Scanner. If you attempt to scan an audio CD the scan will fail.

To scan a CD/DVD and add it to the scanned media file:

1 On the SafeGuard PortProtector Management Server machine run `MediaScanner.exe` from `\Program Files\Sophos\SafeGuard PortProtector\Management Server\tools`, or copy `MediaScanner.exe` to any computer and run it. The following window opens:

2 If you wish to change the default output file name or location, use the Browse button.

Note: If you change the file name, the suffix must remain .XML

3 By default, the Media Scanner is set to append scanned media information to the existing scanned media file. If you wish to add media to a new file, uncheck the **Append to existing file** checkbox.

4 Insert the required media into the CD/DVD drives and click Run. The scanning process begins.

Note: The process scans all media inserted into CD/DVD drives at the time of the scan, meaning you may scan more than one medium in each session.

5 You can view the scan progress in the **Scan Progress** section, which includes the following details:

6 **Drive**: name of the drive in which scanned medium is inserted

7 **Volume Name**: name of the scanned volume, if one has been assigned

8 **Type**: CD or DVD

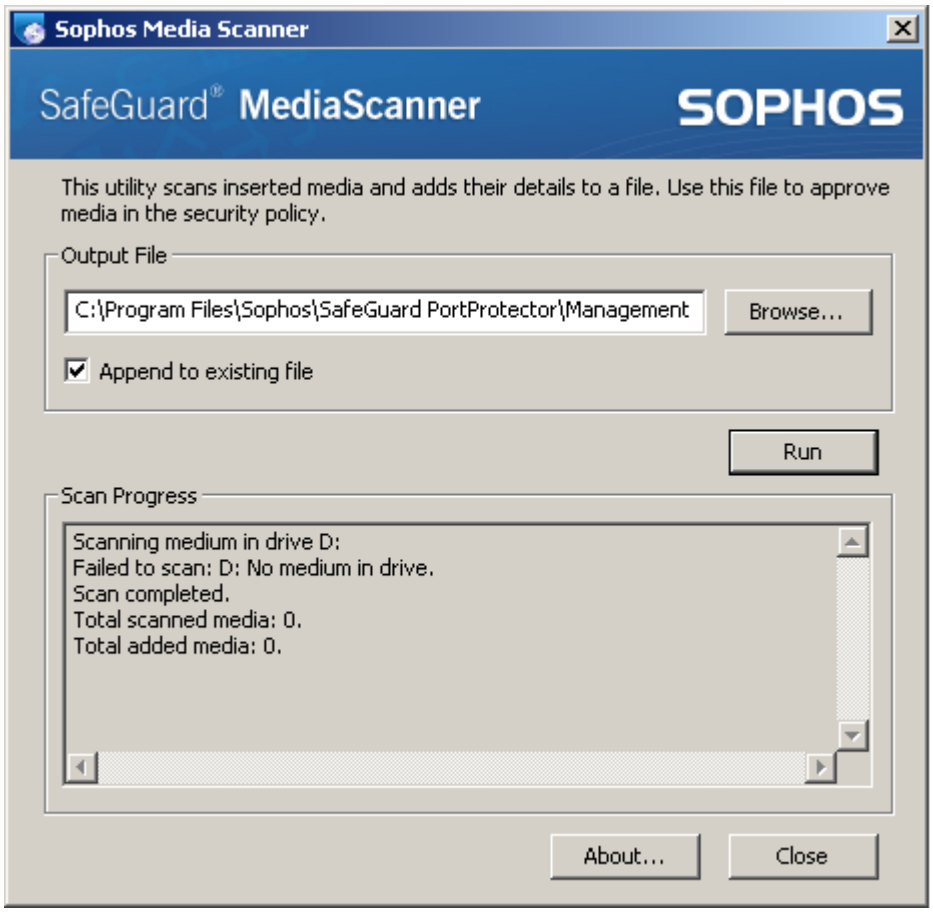
9 **Fingerprint**: a readable version of the fingerprint

10 **Size**: size of the content on the medium

11 **Time**: date and time when scan was performed

Note: If the Scanned media file contains more than one medium, and the volume name is non-existent or is not sufficient in order for you to identify the medium later when adding media to the White List, make sure other details provided in the Scan Progress section are available to you when adding media to the White List (refer to *Approving CD/DVD Media* in *Chapter 3, Defining Policies*). You can also view these details in the scanned Media file, as explained in *Viewing the Scanned Media File* below.

12 Once a scan is completed, the Scan Progress section displays the total of scanned media and the total number of media added to the Scanned Media file, as shown in the following figure.



Note: If a scan fails, a notification appears in the Scan Progress section.

13 Upon completion of a scan, you may repeat the process for additional media by inserting a medium into the CD/DVD drive and clicking Run.

12.2 Viewing the Scanned Media File

If you wish, you may open the Scanned Media file in order to view scan details.

To view the scanned media file contents:

1 Open the file using Microsoft Excel. The file contains one line for each medium, and displays the following columns:

2 **VolumeName**: name of the scanned volume, if one has been assigned

3 **Type**: CD or DVD

4 **Size**: size of the content on the medium

5 **Time**: date and time when scan was performed

6 **ShortFingerprint**: a shorter version of the long fingerprint

7 **LongFingerprint**: the actual fingerprint used by SafeGuard PortProtector

Note: When viewing the file, do not make any changes to it. Modifying the file may later prevent adding the modified medium to the CD/DVD Media White List.

13 Appendix E - Using SafeGuard PortProtector in a HIPAA Regulated Organization

About This Appendix

Recent security breaches and changes in the use of portable and storage technology have prompted the Department of Health and Human Services (DHHS) to require Health Insurance Portability and Accountability Act (HIPAA) regulated organization's (i.e., covered entities) to address data leakage problems. In recognition of the data leakage threat, DHHS has issued specific guidance for the use of portable mobile devices and offsite transport of EPHI such as laptops, PDAs, and USB drives (HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information, Department of Health & Human Services, Centers for Medicare & Medicaid Services, January 8, 2007).

The Privacy and Security Rules of HIPAA requires regulated organizations to protect Electronic Protected Health Information (EPHI). These security rules require organizations to review and modify, when necessary, their formally documented security policies and procedures on a regular basis. Due to concerns over data leakage, DHHS has provided specific guidance for addressing the emerging threat of EPHI disclosure through uncontrolled storage devices and unapproved network access that must be addressed by HIPAA regulated organizations.

SafeGuard PortProtector helps you regain control of your endpoints and address data leakage and targeted attack threats. This chapter provides guidance on how to address these threats within a HIPAA regulated environment.

The first section, *Pre-Requisites for Addressing HIPAA Data Leakage Issues*, examines organizational issues and pre-requisites that must be addressed prior to implementing SafeGuard PortProtector security features and settings. It contains the following sub-sections:

- *Foundations* translate business objectives into a HIPAA compliant context.
- *Considerations* describe the information security threats that must be addressed within the context of the established business mission.
- *Preparations* describes the activities that should be performed before configuring SafeGuard PortProtector for EPHI protection

The second section, *Implementing SafeGuard PortProtector in a HIPAA Regulated Organization*, provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product. It contains the following sub-sections:

- *Implementation Approaches* describes the different implementation approaches suggested in this document.
- *Policy Settings* describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a HIPAA environment.
- *Other SafeGuard PortProtector Settings* describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to the business objectives and the environment of the HIPAA organization.

- *HIPAA Security Rule / SafeGuard PortProtector Feature Mapping* provides additional advice on how SafeGuard PortProtector helps to meet HIPAA Security Rule requirements.

13.1 Pre-Requisites for Addressing HIPAA Data Leakage Issues

SafeGuard PortProtector provides many security features that can address the threats of data leakage and targeted attacks. In order to effectively utilize the capabilities of the product, the HIPAA regulated organization should take some preliminary actions to prepare to use SafeGuard PortProtector for HIPAA compliance.

There are three categories of pre-requisites that help to ensure effective SafeGuard PortProtector implementation for HIPAA compliance. The first category is *Foundations*. Foundations are basic information security program elements that must be in place in order for any compliance effort to move forward. Foundations include the establishment of business mission statements, and roles, responsibilities required to carry them out. The second pre-requisite is *Considerations*. Considerations are specific information security threats that must be addressed within the context of the established business mission. In this case considerations are specific issues regarding the protection of EPHI in light of data leakage threats. The third pre-requisite for effective implementation is *Preparations*. Preparations are activities that must be performed prior to installing and configuring a specific technology product such as SafeGuard PortProtector.

13.1.1 Foundations

The implementation of new technology into an organization requires a context of business objectives. For HIPAA regulated organizations that context is provided by the following set of foundations that translate business objectives into a HIPAA compliant context for the implementation of technology.

Foundation 1 - HIPAA Compliance Program:

A well developed HIPAA compliance program will have implemented a business cycle of review (through risk assessment) and revision of formally documented security policies, procedures, and safeguards. Without such a program the implementation of technology is driven by a limited set of objectives focusing solely on information technology issues. For these reasons it is important to have a strong HIPAA compliance program, supporting business objectives, in place before tailoring the settings of any safeguard to comply with HIPAA requirements.

Foundation 2 - Understand Business Needs:

The decision to expose EPHI to data leakage threats through the use of portable mobile devices and EPHI offsite transport should be based on the neccessity of implementing business objectives. There are a variety of business objectives that may lead to the decision to allow the use of portable mobile devices and offsite transport such as home healthcare, use of PDAs in healthcare applications, or transport of medical information to offsite storage. Such a variety of business objectives leads to a variety in formally documented security policies and the application and configuration of technologic controls. These formal policies are therefore tailored to business objectives and drive the implementation of technology.

13.1.2 Considerations

To protect EPHI security and privacy from unauthorized access, there are a variety of security safeguards (administrative, physical, and technical) that can be used. A coordinated integration of combined safeguards is required to properly protect EPHI. The DHHS security guidance for remote use and access describes several considerations for safeguard enhancement to address this issue. Each of these "considerations" is described below as a recommended element of the HIPAA compliance program to be implemented along with the installation and configuration of SafeGuard PortProtector. Within the description of each of these considerations a set of instructions is also provided to assist in the preparation of SafeGuard PortProtector integration and configuration.

Consideration 1 - Policies and Procedures:

A formally documented security policy is a statement of management's intent for protecting corporate assets from fraud, waste, and abuse. With the emergence of the data leakage threat data access policies and procedures must be reviewed and revised. The principle of least privilege, which states that each user / device should be granted only the level of access required to perform the job, needs to be interpreted to address portable media and devices.

Instructions:

- Ensure that your current policies are based on the principle of "Default – No Access". This principle dictates that by default all users have no access to any corporate resources. If no such policy statement exists – create one.
- Develop guidance that interprets the "Default – No Access" policy and the "Least Privilege" policy to the roles within your organization and to the computing devices within your organization.
- Develop procedures for handling exceptions to the policies. These exceptions will be based on operational needs such as media backup, data transfer, and remote access to networks for telecommuting. Each procedure should address the risk through compensating controls such as policy, sanctions, asset tracking, multi-factor authentication, oversight, and encryption.

Consideration 2 - Training:

Effective security awareness and training is an important element of EPHI protection. HIPAA security and privacy training programs need to be periodically updated to reflect changes in threats and organizational policies. A project to update security awareness and training program should be part of the overall data leakage risk mitigation project.

Instructions:

- Update annual security awareness training and periodic security awareness reminders to include a discussion of data leakage threats, updated policies, user actions required, behavior prohibited, and devices restricted.
- WiFi Threats: use on unapproved networks, rogue networks, hybrid network bridging
- Mobile / Storage Device Threats: physical loss, data removal, malicious code insertion

Consideration 3 - Incident Response.

In the event of a security breach, resulting in the disclosure of EPHI, HIPAA regulated organizations are required to have formally documented security policies, procedures, and the capability of investigating the incident. As the set of possible security incidents expands to include data leakage, organizations must update their policies, procedures, and capabilities to respond to these incidents.

Instructions:

- Update incident response procedures to address data leakage issues. Specifically, create procedures for the following incident types.
- Lost or stolen mobile / storage device
- Found rogue network
- Found hybrid network bridging
- Unapproved data removal

13.1.3 Preparations

SafeGuard PortProtector allows organizations to control access and protect endpoints based on user roles, network domains, computer types, and criticality of systems and data. The specific implementation and configuration of SafeGuard PortProtector requires an accurate knowledge of objects SafeGuard PortProtector is to protect, the formally documented security policies it is to enforce, and the administrative roles that will maintain the SafeGuard PortProtector software. The following activities are an important element of the preparation to install and configure SafeGuard PortProtector for EPHI protection.

Preparation 1 - Determine Endpoint Protection Needs:

SafeGuard PortProtector protects endpoints of your network from data leakage and targeted attacks. SafeGuard PortProtector provides the ability to lock down these endpoints from data leakage through physical ports and devices and a variety of attacks and vulnerabilities. On the other hand your organization has a variety of business needs that will require connectivity to external storage devices, wireless networks, and other possible threats. In preparation for a SafeGuard PortProtector deployment your organization should determine the protection and business needs of the endpoints.

Instructions:

- Update endpoint inventory and classification. Be sure that you are aware of all your endpoints within your network that store, process, or transmit EPHI. This can be done through a manual inventory process or through the use of directory services. Classification is based on your data classification policy and includes a classification of endpoints that handle EPHI data.
- Scan each endpoint to detect port, device, and WiFi usage. The SafeGuard PortAuditor will automatically detect devices and networks that are currently or previously connected.
- Review your “Default – No Access” and “Least Privilege” policies as they apply to the endpoints that have now been inventoried, classified, and scanned. Make a list of the intended profiles for each endpoint classification.

Preparation 2 - Determine User Access Roles

SafeGuard PortProtector allows for the specification of allowed ports, devices, and WiFi usage according to user, user group, or organizational unit as defined by Active Directory or Novel eDirectory. It is important to note that any user privileges granted through this mechanism will trump those specified for an individual endpoint. For example, if you set up a user to have WiFi access and have also locked down a laptop to block WiFi access through SafeGuard PortProtector, that user will be able to gain WiFi access through that laptop based on his SafeGuard PortProtector user profile. With this rule in mind it is strongly recommended that you be very careful when creating any user privileges. User privileges will supersede any restrictions placed on endpoints.

Instructions:

- Determine user roles within your SafeGuard PortProtector implementation.
- User – this role is the normal user role that has no additional privileges other than the privileges that are common throughout the organization.
- Privileged user – this role has extended privileges (for example - the ability to write files to a USB device or connect to a WiFi network).
- Determine compensating controls placed on privileged users.
- Logs and alerts – at a minimum plan to set privileged user policies to log allowed behavior that is extended from the normal user role. Consider setting alerts on highly sensitive behavior such as connecting an external hard disk.

Preparation 3 - Determine Administration Roles

SafeGuard PortProtector allows for multiple administration roles according to roles and organizational structure. The use of these administrative role options should be determined prior to installation of SafeGuard PortProtector.

Instructions:

- Determine if your implementation of SafeGuard PortProtector will follow a centralized or de-centralized administration model.
- Centralized – a single entity is responsible for the administration of SafeGuard PortProtector.
- De-centralized – administration of SafeGuard PortProtector is delegated to departments that are responsible for the administration of their own part of the domain. If you chose this method of administration, then determine the domain partitions for which each department will be responsible for the administration.
- Determine administration roles within each domain.
- The SafeGuard PortProtector administrator may be set up as a single role or you may delegate administrative privileges to implement separation of duties. Determine the set of administrative roles that you will implement.
- Plan maintenance and incident response function for SafeGuard PortProtector administration.
- Incident response – those responsible for responding to incidents involving lost or stolen storage devices, rogue networks, hybrid network bridging, or unapproved data removal will require special permissions within SafeGuard PortProtector and access to audit tools. Document the incident response roles within your organization and the permissions and access required.

- Maintenance – those responsible for handling end user issues such as peripherals and network connectivity will require the ability to request modifications to object or user permissions. Document maintenance roles within your organization and the permissions and access required.

13.2 Implementing SafeGuard PortProtector in a HIPAA Regulated Organization

This section provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product.

- *Implementation Approaches* describes the various implementation approaches suggested in this document.
- *Policy Settings* describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a HIPAA environment.
- *Other SafeGuard PortProtector Settings* describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to the business objectives and the environment of the HIPAA organization.
- *HIPAA Security Rule / SafeGuard PortProtector Feature Mapping* provides additional advice on how SafeGuard PortProtector helps to meet HIPAA Security Rule requirements.

13.2.1 Implementation Approaches

The HIPAA Security Rule requires HIPAA regulated organizations to protect EPHI through a set of required and addressable standards (The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334). However, the HIPAA Security Rule does not specify precisely how to implement these safeguards or what mechanisms must be employed. Since each organization has its own unique business objectives, there will be a variety of HIPAA implementations throughout the HIPAA regulated organization community. In an effort to address these differing implementations this document provides guidance for both a "Standard" and an "Aggressive" approach for implementing SafeGuard PortProtector to protect EPHI. Both of these approaches meet the HIPAA standards for the requirements they address.

Standard Approach: The standard approach to implementing SafeGuard PortProtector within a HIPAA environment implements good security practices for protecting endpoints from targeted attacks and ensuring that potential data leakage of EPHI is monitored and logged.

Aggressive Approach: The aggressive approach to implementing S SafeGuard PortProtector within a HIPAA environment implements a more strict set of security practices for protecting endpoints from targeted attacks and ensuring that potential data leakage of EPHI is blocked, encrypted, or monitored and logged.

The selection of the appropriate approach for meeting both HIPAA and an organization's business objectives maybe either the Standard Approach, the Aggressive Approach, or even a combination or customization of either of these approaches. Recall "Foundation 2: Understand Business Needs" (*see above*) from part 1 of this whitepaper, which stresses the importance of understanding the business objectives and environment in which SafeGuard PortProtector is to be deployed prior to determining the configuration and setting of the product. Just as technology implementation to meet HIPAA requirements is flexible, so is the configuration of SafeGuard PortProtector. The flexibility is designed to meet the variety of business objectives of HIPAA regulated organizations.

13.2.2 Policy Settings

The following table is a guide to the SafeGuard PortProtector administrator in the setting and configuration of SafeGuard PortProtector for implementation within a HIPAA environment. The standard and aggressive approaches are to be used as guidelines for setting the parameters of SafeGuard PortProtector and not to be interpreted as additional HIPAA requirements. In fact the HIPAA security rule does not specify protection requirements down to this level of detail. However, these configuration settings do follow general security principles and can be used as a baseline in creating a policy set for your own organization.

Setting	Standard HIPAA Approach	Aggressive HIPAA Approach	Rationale
Policy		Create new policies based on the built-in policy of Standard HIPAA or Aggressive HIPAA. Each policy can then be modified as determined by the HIPAA compliance officer and in accordance with the organization's business objectives.	
Port Control:			
USB	Restrict	Restrict	Restricting access to these ports allows for a finer granularity of control under the device control section of the policy-security.
FireWIre	Restrict	Restrict	
PCMCIA	Restrict	Restrict	
SD	Allow	Allow	Allowing access to these ports is required for some standard human interface devices. The access restrictions to these ports for storage devices will be further restricted through storage control below.
Serial	Allow	Allow	
Parallel	Allow	Allow	
WiFi	Restrict	Restrict	Restricting access to WiFi networks allows for a finer granularity of control under the WiFi control section of the policy-security.
Modem	Allow + log	Allow + log	Use of Modem, IrDA, or Bluetooth can lead to unauthorized network connections. At a minimum use of these ports should be logged. A more aggressive posture would block and log IrDA and Bluetooth links.
IrDA	Allow + log	Block + log	
Bluetooth	Allow + log	Block + log	

Setting	Standard HIPAA Approach	Aggressive HIPAA Approach	Rationale
Network Bridging	Block (All)	Block (All)	Blocking user access to WiFi, Bluetooth, Modems, and IrDA links while connected to the TCP/IP network interface protects endpoints from the dangerous practice of hybrid network bridging.
Device Control			
Hardware Keyloggers	Allow	Allow	Although the use of hardware keyloggers should be restricted and users should be protected from these attacks, usability concerns override the need for this restriction.
Human Interface	Allow	Allow	It is typically not considered a risky practice to allow users to connect to human interface devices such as keyboards and mice.
Printers	Allow	Allow	Although a printer can be a data leakage source, printing is a common user function within most organizations. Compared to storage devices and PDAs, printers have a much lower capacity to "leak" large amounts of EPHI. This risk can be mitigated by physical and administrative controls.
PDA	Allow + Log	Restrict, White List, Log	PDAs, mobile phones, Imaging devices (such as scanners) and Audio / Video devices (such as MP3 players) present a
Mobile Phones			
Imaging			

Setting	Standard HIPAA Approach	Aggressive HIPAA Approach	Rationale
Audio / video Devices			clear risk to the control and protection of EPHI. At a minimum a HIPAA organization should log any such behavior. A more aggressive setting to not only log the behavior but restrict use to an approved list of devices such as company issued PDAs.
Network Adapters	Allow	Allow	Network adapters allow the PC to be connected to a network. This is a common configuration and should not be blocked or logged.
Smart Cards	Allow	Allow	Smart Cards are common as an authentication device. They do not pose a reasonable threat to EPHI data.
Content security devices	Allow	Allow	Content security devices monitor the content of the flow of data to and from the endpoint. If such devices are present they are part of a solution to enforce security and should not be blocked at the endpoint.
Unclassified devices	Block + Log	Block + Log	Unclassified devices are any devices that are not otherwise specified. These should not turn up very often, and present a risk to EPHI control and protection.
Storage Control			
Autorun function	Block	Block	A convenience feature of many operating systems is the ability to automatically execute a program upon the

Setting	Standard HIPAA Approach	Aggressive HIPAA Approach	Rationale
			insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat and should be disabled by default.
Removable storage	Allow + log Block smart function	Encrypt + log Block smart function	Storage devices (such as USB drives) present a clear risk to EPHI control and protection. At a minimum a HIPAA organization should log use of storage devices. A more aggressive approach would restrict the use of storage devices to approved devices. A more aggressive approach would also ensure that EPHI written to storage devices is encrypted; providing further protection in the event the storage device is lost or stolen. Certain formats for writing files to media such as CD or DVD do not support the event logging. In the aggressive HIPAA setting to preserve the logging settings for all files this option should remain checked.
External HD	Allow + log	Encrypt + log	
CD/DVD	Allow + log Allow unsupported formats	Encrypt + log Block unsupported formats	
Floppy Drives	Allow + log	Read only + log	
Tape Drives	Allow + log	Restrict + log	
File Control	Allow + Log (write only)	Allow + Log (write only)	In order to support audit and investigation of security incidents involving EPHI log all files written to external storage devices.
WiFi Network	Allow + Log	Restrict networks, block peer to peer, White List	Wireless networks present a clear risk to the control and protection of EPHI. At a minimum a HIPAA

Setting	Standard HIPAA Approach	Aggressive HIPAA Approach	Rationale
			organization should log any such behavior. A more aggressive setting to not only log the behavior but restrict use to an approved list of WiFi networks that have been approved by the organization and have proper encryption.
Policy Settings			
Logging	Send logs to SafeGuard PortProtector Server Send logs every 12 hours or less. Log connect and disconnect events	Send logs to SafeGuard PortProtector Server Send logs every 12 hours or less. Log connect and disconnect events	Logs should clearly not be stored on the endpoint, but instead sent to the SafeGuard PortProtector Server where they can be protected and viewed by the administrator. Other logging settings here provide adequate EPHI protection by ensuring periodic updating of logs on the server without burdening the network; inclusion of connect and disconnect events to allow for analysis of how long a device was connected;
End-user messages	Review the end user messages associated with the HIPAA setting to ensure they are consistent with your formally documented security policies and security awareness training program.		It is important to provide a constant reminder to those exposed to EPHI that they are responsible for protecting EPHI and complying with policies. Modifying the end-user messages to specifically mention HIPAA security and EPHI protection will assist in the security awareness of your organization.

Setting	Standard HIPAA Approach	Aggressive HIPAA Approach	Rationale
Encryption	None	Do not allow users to access encrypted devices at home Approve read only access for non-encrypted devices.	It is important to restrict the use of EPHI to systems with adequate protection measures. Home computers generally lack HIPAA required security controls. Setting read-only for non-encrypted devices allows the flexibility of importing information without exposing EPHI to the risk of disclosure from loss or theft of a non-encrypted device.
Options	Use a different password from the client administration password to uninstall SafeGuard PortProtector Full visibility on endpoints	Use a different password to uninstall SafeGuard PortProtector Full visibility on endpoints	In order to enforce the principle of separation of duty and general password security, use a different password for the uninstall process of SafeGuard PortProtector Client than the client administration password. Consistent with the advice under “end user messages” it is best to let users know about the protections SafeGuard PortProtector is providing to EPHI.

13.2.3 Other SafeGuard PortProtector Settings

For the appropriate setting of other SafeGuard PortProtector features and options refer to *Pre-Requisites for Addressing HIPAA Data Leakage Issues* detailed in part 1 of the HIPAA Security Compliance with SafeGuard PortProtector document. Specifically, the following SafeGuard PortProtector features should follow the business objectives and the environment of the HIPAA organization as defined in foundations, considerations, and preparations.

Alerts

SafeGuard PortProtector alerts provide oversight of administrative actions and protection of the SafeGuard PortProtector security functions in case of attempted tampering. The following alert options should be set in order to preserve the security functions provided by SafeGuard PortProtector:

Log all administrative events: Logs all administrative actions and provides oversight of SafeGuard PortProtector administration.

Alert all tempering events: Detects tempering attempts and ensures the integrity of end point protection controls.

SafeGuard PortProtector Administration

SafeGuard PortProtector may be run by a single administrator or an organization may implement additional access control by defining additional administrators to a subset of administrative functions. This is an implementation of role-based access control and should be considered based on the organizations approach as defined in "Preparation 3: Determine Administrative Roles." Among the roles a HIPAA organization should consider are the following:

- Log Reviewer: Access to all logs and log functions without ability to edit policies.
- Policy Administrator: Access to edit and administer policies without ability to view logs.
- Audit: Read-only access to administrators console without ability to perform any changes.

The setting of these roles should be based on the administration model and approach of the organization and the support needed for incident response and maintenance. Refer to Part 1 of this whitepaper for more complete instructions for SafeGuard PortProtector implementation *Preparations*.

Domain Partitioning

Further access control granularity may be added with the SafeGuard PortProtector domain partitioning feature. The role based access mechanism includes domain partitioning, which allows an administrator role to be limited to a specific group of clients. This feature is useful in restricting the administrator's access to sensitive domains such as those domains which contain EPHI. The setting of these roles should be based on the organization's administration model and approach and the support needed for incident response and maintenance. Refer to Part 1 of this whitepaper for more complete instructions for the SafeGuard PortProtector implementation preparation.

Administrative Password Strength

All passwords that protect EPHI within a HIPAA organization must comply with the organization's formally documented password policies. Formally documented security policies are discussed in more detail in "Consideration 1: Policies and Procedures" in part 1 of this document. Based on the organization's password strength policy, SafeGuard PortProtector administrative password strength criteria should be defined in the SafeGuard PortProtector to enforce organizational policies. Elements of the password strength include minimum length and required character types.

13.2.4 HIPAA Security Rule / SafeGuard PortProtector Feature Mapping

SafeGuard PortProtector provides HIPAA organizations additional technical controls to protect EPHI at system endpoints and address data leakage and target attack threats. As discussed throughout this paper SafeGuard PortProtector can address data leakage risks, targeted attack threats, and many of the HIPAA Security Rule requirements. Although obvious, it should be noted that SafeGuard PortProtector provides a portion of the technical controls (and influences some administrative controls) necessary for complete HIPAA compliance. The table below provides additional advice on how SafeGuard PortProtector helps to meet HIPAA Security Rule requirements.

HIPAA			
Section of HIPAA Security Rule	Rule Description	Relevant SafeGuard PortProtector Features	How to Satisfy HIPAA Controls with SafeGuard PortProtector
Physical Safeguards			
164.310(d)(1)	Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	SafeGuard PortProtector provides the ability to control access to portable storage devices such as USB drives, PDAs, and mobile phones. The flexibility of SafeGuard PortProtector policies allow for a granularity of control that matches a HIPAA organization's needs. Options include the ability to record connection and disconnection of devices and media.	Configure SafeGuard PortProtector to control media and storage device use on the organization's desktops and laptops. Two built-in HIPAA approaches provide reasonable approaches and rationale for these settings. Review logs according to organization policy and procedures.

IPAA			
Section of HIPAA Security Rule	Rule Description	Relevant SafeGuard PortProtector Features	How to Satisfy HIPAA Controls with SafeGuard PortProtector
Administrative Controls			
164.308(a)(1)(i)	Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	SafeGuard PortProtector is a technology control that can implement policies and procedures to prevent and detect security violations at the network endpoints.	See consideration 1 [Policies and Procedures] for instructions on what policies and procedures need to be implemented. SafeGuard PortProtector has built-in security policies for “Standard HIPAA Approach” and “Aggressive HIPAA Approach”. Associate built-in policies for either HIPAA approach with your users and machines that may have EPHI access. If your organization chooses to deviate from built-in HIPAA policies, document business reason and compensating controls.

164.308(a)(1)(ii)(A)	Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the organization.	SafeGuard PortAuditor provides a full view of the ports, devices and networks in use by your organization's users, as well as a history of what was used previously. The SafeGuard PortAuditor scan output can select the devices and networks to control. Left uncontrolled, all of these devices provide vulnerability for the misuse of EPHI.	Utilize SafeGuard PortAuditor during the data gathering phase. Specifically, scan all endpoints for current settings (ports, peripherals, etc.) and port and device usage history. Review scan results against the current policies covering endpoint security. The data leakage threat can be measured during a risk assessment by temporarily applying a policy of “allow + log”. The results could be reviewed to determine the current extent of data transfer to storage devices.

164.308(a)(1)(ii)(D)	Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	SafeGuard PortProtector products collect several logs types: Client Log – Information about Clients and users in the organization. Each record reports a specific event, such as the connection of a detachable device to a computer, or a tampering attempt. File Log – File information for removable storage devices, external hard disks or CD/DVD Server Log – Information about the Management Server and administrative actions. Each record reports a specific event, such as logging into the Management Console, and changing Global Policy Settings.	Configure SafeGuard PortProtector to collect logs and send alerts according to your organizations policy. Two built-in HIPAA approaches provide reasonable approaches and rationale for these settings. Review logs according to organization policy and procedures.

HIPAA			
Section of HIPAA Security Rule	Section of HIPAA Security Rule	Section of HIPAA Security Rule	Section of HIPAA Security Rule
Technical Safeguards			
164.312(a)(2)(iv)	Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information.	Using the policy manager, user behavior is controlled at the endpoint. Depending on the connected device, SafeGuard PortProtector can force all information directed to a specific device to be encrypted. As a rule, organizationally-encrypted removable storage devices can be used only when connected to protected endpoints. An optional function allows or prohibits content from being opened on non-organizational computers. For Non-encrypted Devices, policies can be deployed that determine behavior when a non-encrypted device is detected; the device may either be blocked, or permitted Read Only access. Wireless networks can be controlled at the endpoint. Two types of control are available: Specify which connection types are allowed access Determine which specific networks are allowed access.	SafeGuard PortProtector extends the ability to enforce encryption policies and procedures within a HIPAA organization. SafeGuard PortProtector can enforce these procedures by blocking attempts to read or write unencrypted devices, and guide the user in the process of encrypting an unencrypted device. blocking the use of encrypted devices outside the organization ensuring wireless communication is restricted to properly encrypted and approved wireless networks.

164.312(b)	Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI	SafeGuard PortProtector records endpoint events associated with storage devices and media in client logs. An event may be a device connection or disconnection, a wireless network connection, tampering attempts or administrator login. Event logs include endpoint identify, user, event type, and time. SafeGuard PortProtector also creates server logs for administrative events such as administrator login, publishing policies and performing backups. Client and Server logs are sent to a log repository and stored on the Management Server at the defined intervals.	Configure SafeGuard PortProtector to collect client and server logs according to your organizations policy. Built-in management, operational, and audit reports collect and organize critical data that allows for the efficient examination of activities related to data transfer to storage devices and media.
164.312(e)(2)(ii)	Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Policies can be created that either force data to be encrypted before being transferred to removable storage devices, or force the use of encrypted WiFi channels for secure transfer of data.	SafeGuard PortProtector extends the ability to enforce encryption policies and procedures within a HIPAA organization. blocking attempts to write to unencrypted devices blocking the non-network use of encrypted devices ensuring wireless communication is restricted to properly encrypted and approved wireless networks.

14 Appendix F – Using SafeGuard PortProtector in a SOX Regulated Organization

About This Appendix

In response to the major corporate accounting scandals at the beginning of the millennium, the United States enacted a public law entitled "Public Company Accounting Reform and Investor Protection Act of 2002." This law is generally referred to by its shorter nickname in honor of the major sponsors of the act, Senator Paul Sarbanes (D-MD) and Representative Michael Oxley (R-OH), thus Sarbanes-Oxley or SOX. The law contains many titles and provisions but the area of most concern regarding information security is section 404: Assessment of internal control.

SOX section 404 requires, among other things, for an external auditor to evaluate the controls for safeguarding assets. This review of controls by an external auditor is typically guided by the Common Objectives of Information and Related Technology (COBIT) as an internal control framework. Recent data losses and attacks at the endpoint have highlighted the need for protection at all levels of the network, including network endpoints. Ensuring security at the endpoints within a network is one of the issues that must be addressed by all organizations seeking to meet SOX requirements.

SafeGuard PortProtector helps you regain control of your endpoints and address data leakage and targeted attack threats. This chapter provides guidance on how to address these threats within a SOX 404 regulated environment.

The first section *Pre-Requisites for Addressing SOX Compliance Issues*, examines organizational issues and pre-requisites that must be addressed prior to implementing SafeGuard PortProtector security features and settings. It contains the following sub-sections:

- *Foundations* translates business objectives into a SOX compliant context.
- *Considerations* describes the information security threats that must be addressed within the context of the established business mission.
- *Preparations* describes the activities that should be performed before configuring SafeGuard PortProtector for protection.

The second section, *Implementing SafeGuard PortProtector in a SOX Regulated* Organization, provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product. It contains the following sub-sections:

- *Implementation Approaches* describes the different implementation approaches suggested in this document.
- *SOX policy settings* describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a SOX environment.
- *Other SafeGuard PortProtector SOX Settings* describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to the business objectives and the environment of the SOX organization.

- *Relevant SOX Requirements* provides additional information on SOX Security Rule requirements.

14.1 Pre-Requisites for Addressing SOX Compliance Issues

SafeGuard PortProtector provides many security features that can address the threats of endpoint security. In order to effectively utilize the capabilities of the product, the SOX regulated organization should take some preliminary actions to must prepare to use SafeGuard PortProtector for SOX 404 compliance.

There are three categories of pre-requisites for effective implementation of SafeGuard PortProtector for SOX 404 compliance. The first category is *Foundations*. Foundations are basic information security program elements that must be in place in order for any compliance effort to move forward. Foundations include the establishment of business mission statements, and roles, responsibilities required to carry them out. The second pre-requisite is *Considerations*. Considerations are specific information security threats that must be addressed within the context of the established business mission. The third pre-requisite for effective implementation is *Preparations*. Preparations are activities that must be performed prior to installing and configuring a specific technology product such as SafeGuard PortProtector.

14.1.1 Foundations

The evaluation of security controls within an organization requires a context of business objectives. For SOX regulated organizations that context is provided by the following set of foundations that translate business objectives into a SOX 404 compliant context for the implementation of technology.

Foundation 1: Information Security Program

An information security program consists of dedicated security professionals supported by management with the appropriate scope, authority, and budget to assess information security risks, recommend mitigation techniques and ensure appropriate security risk management of the organization's assets. A strong information security program will include an identification of reasonable threats to the organization's assets, a review of the physical, administrative, and technical controls, and the planning and implementation oversight of security controls to bring the security posture to an acceptable assurance level.

Foundation 2: Audit Program

An organization seeking to comply with SOX must have an existing internal audit program. Such a program comprises the policies and procedures that govern the internal audit function. At a minimum an internal audit program includes an audit charter (establishing the audit function), annual risk assessments, an audit plan (goals, schedules, and staffing for audit), and audit processes for the audit cycle, audit efforts, audit reports, and audit documentation.

14.1.2 Considerations

To ensure the protection of the organization's assets there are a number of control objectives that must be met. Prior to embarking on an effort to implement these control objectives SOX organization should first consider several key elements of the upcoming SOX 404 compliance project. Careful consideration of these elements can help an organization avoid several common pitfalls and increase its efficiency in the SOX 404 compliance effort.

Consideration 1: Control Objectives

Common Objectives of Information and Related Technology (COBIT) is an internal control framework used as a guide by external auditors to review the effectiveness of the controls on your internal financial systems. It is important to remember that COBIT is a guide and can be tailored to meet your business objectives by choosing appropriate control objectives and compensating controls where applicable. Work with your external audit team to develop the appropriate set of control objectives for your organization. As the COBIT and the audit process can seem foreign to many within the IT department, the addition of a Certified Information System Auditor (CISA) to your internal team overseeing the external audit can create efficiencies in your SOX 404 compliance project.

Instructions:

- Work with external audit team to develop an appropriate set of control objectives.
- Review reasonableness and completeness of proposed control objectives.
- Add a Certified Information System Auditor (CISA) to your internal team working with the external auditors.

Consideration 2: Policies and Procedures

A security policy is a statement of management's intent for protecting corporate assets from fraud, waste, and abuse. With the emergence of the data leakage threat data access policies and procedures must be reviewed and revised. The principle of least privilege, which states that each user should be only the level of access required to perform their job, needs to be interpreted to address portable media and devices.

Instructions:

- Ensure that your current policies are based on the principle of "Default – No Access". This principle dictates that by default all users have no access to any corporate resources. If no such policy statement exists – create one.
- Develop guidance that interprets the "Default – No Access" policy to the roles within your organization and to the computing devices within your organization.
- Develop procedures for handling exceptions to the "Default – No Access" policy. These exceptions will be based on operational needs such as media backup, data transfer, and remote access to networks for telecommuting. Each procedure should address the risk through compensating controls such as policy, sanctions, asset tracking, multi-factor authentication, oversight, and encryption.

Consideration 3: Training

Effective security awareness and training is an important element of asset protection. Information security training programs need to be periodically updated to reflect changes in threats and organizational policies. A project to update security awareness and training program should be part of the overall data leakage risk mitigation project.

Instructions:

- Update annual security awareness training and periodic security awareness reminders to include a discussion of data leakage threats, updated policies, user actions required, behavior prohibited, and devices restricted.
- Wi-Fi Threats: use on unapproved networks, rogue networks, hybrid network bridging, WEP authentication.
- Mobile / Storage Device Threats: physical loss, data removal, malicious code insertion

Consideration 4: Incident Response

In the event of a security breach resulting in the disclosure, modification, or interruption of service, SOX 404 compliant organizations are required to have policies, procedures, and the capability of investigating the incident. As the set of possible security incidents expands to include data leakage, organizations must update their policies, procedures, and capabilities to respond to these incidents.

Instructions:

- Update incident response procedures to address data leakage issues. Specifically, create procedures for the following incident types.
- Lost or stolen mobile / storage device
- Found rogue network
- Found hybrid network bridging
- Unapproved data removal

14.1.3 Preparations

SafeGuard PortProtector allows organizations to control access and protect endpoints based on user roles, network domains, computer types, and criticality of systems and data. The specific implementation and configuration of SafeGuard PortProtector requires an accurate knowledge of objects SafeGuard PortProtector is to protect, the policies it is to enforce, and the administrative roles that will maintain the SafeGuard PortProtector software. The following activities are an important element of the preparation to install and configure SafeGuard PortProtector the implementation of appropriate internal controls.

Preparation 1: Determine Endpoint Protection Needs

SafeGuard PortProtector provides the ability to protect stored data for uncontrolled export on removable devices at endpoints. On the other hand your organization has a variety of business needs that will require connectivity to external storage devices, wireless networks, and other possible threats. In preparation for a SafeGuard PortProtector deployment your organization should determine the protection and business needs of the endpoints.

Instructions:

- Update endpoint inventory and classification. Be sure that you are aware of all the endpoints within your network that store, process, or transmit sensitive data. This can be done through a manual inventory process of through the use of directory services. Classification is based on your data classification policy and includes a classification of endpoints that handle sensitive data.
- Scan each endpoint to detect port, device, and Wi-Fi usage. The SafeGuard PortAuditor utility will automatically detect devices and networks that are currently or previously connected.
- Review your "Default – No Access" and least privilege policies as they apply to the endpoints that have now been inventoried, classified, and scanned. Make a list of the intended profiles for each endpoint classification.

Preparation 2: Determine User Access Roles

SafeGuard PortProtector allows for the specification of allowed ports, devices, and Wi-Fi usage according to user, user group, or organizational unit as defined by Active Directory or Novel eDirectory. It is important to note that any user privileges granted through this mechanism will trump those specified for an individual endpoint. For example, if you set up a user to have Wi-Fi access (over WPA networks) and have also locked down a laptop to block Wi-Fi access, that user will be able to gain Wi-Fi access through that laptop. With this rule in mind it is strongly recommended that you be very careful when creating any user privileges as those privileges will apply to any endpoint to into which that user logs.

Instructions:

- Determine user roles within your SafeGuard PortProtector implementation.
- User – this role is the normal user role that has no additional privileges associated.
- Privileged user – this role has extended privileges such as the ability to write files to a USB device or connect to a WPA-enabled Wi-Fi network.
- Determine compensating controls placed on privileged users.
- Logs and alerts – at a minimum plan to set privilege user policies to log allowed behavior that is extended from the normal user role. Consider setting alerts on highly sensitive behavior such as connecting and external hard drive.

Preparation 3: Determine Administration Roles

SafeGuard PortProtector allows for multiple administration roles according to privilege and domain. The use of these administrative role options should be determined prior to installation of SafeGuard PortProtector.

Instructions:

- Determine if your implementation of SafeGuard PortProtector will follow a centralized or de-centralized administration model.
- Centralized – a single entity is responsible for the administration of SafeGuard PortProtector.
- De-centralized – administration of SafeGuard PortProtector is delegated to departments that are responsible for the administration of their own domain. If you chose this method of administration, then determine the domain partitions for which each department will be responsible for the administration.
- Determine administration roles within each domain.
- The SafeGuard PortProtector administrator may be set up as a single role or you may delegate administrative privileges to implement separation of duties. Determine the set of administrative roles that you will implement.
- Plan maintenance and incident response function for SafeGuard PortProtector administration.
- Incident response – those responsible for responding to incidents involving lost or stolen storage devices, rogue networks, hybrid network bridging, or unapproved data removal will require special permissions within SafeGuard PortProtector and access to audit tools. Document the incident response roles within your organization and the permissions and access required.
- Maintenance – those responsible for handling end user issues such as peripherals and network connectivity will require the ability to request modifications to object or user permissions. Document maintenance roles within your organization and the permissions and access required.

14.2 Implementing SafeGuard PortProtector in a SOX Regulated Organization

This section provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product.

- Implementation Approaches describes the different implementation approaches suggested in this document.

- *SOX policy settings* describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a SOX regulated environment.
- *Other SafeGuard PortProtector SOX Settings* describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy.
- *Relevant SOX Requirements* provides additional information on the SOX Security Rule requirements.

14.2.1 Implementation Approaches

The SOX 404 / COBIT regulation requires SOX regulated organizations to provide adequate internal controls. However, the SOX 404 / COBIT does not specify precisely how to implement these safeguards or what mechanisms must be employed. Since each organization has its own unique business objectives, there will be a variety of COBIT implementations throughout the SOX regulated organization community]. In an effort to address these differing implementations this document provides guidance for both a "Standard" and an "Aggressive" approach for implementing SafeGuard PortProtector to protect the organization's assets. Both of these approaches meet the SOX 404 / COBIT standards for the requirements they address.

Standard Approach: The standard approach to implementing SafeGuard PortProtector within a SOX regulated environment implements good security practices for protecting endpoints from targeted attacks and ensuring that adequate internal controls for the protection of data leakage at network endpoints.

Aggressive Approach: The aggressive approach to implementing SafeGuard PortProtector within a SOX regulated environment implements a more strict set of security practices for protecting endpoints from targeted attacks and ensuring adequate internal controls for the protection of data leakage at network end points.

The selection of the appropriate approach for meeting both SOX 404 / COBIT and an organization's business objectives maybe either the Standard Approach, the Aggressive Approach, or even a combination or customization of either of these approaches. Recall "Consideration 1: Control Objectives" under *Considerations,* which stresses the importance of understanding the business objectives and environment in which SafeGuard PortProtector is to be deployed prior to determining the configuration and setting of the product. Just as technology implementation to meet SOX 404 / COBIT requirements is flexible, so is the configuration of SafeGuard PortProtector. The flexibility is designed to meet the variety of business objectives of SOX regulated organizations.

14.2.2 SOX policy settings

The following table is a guide to the SafeGuard PortProtector administrator in the setting and configuration of SafeGuard PortProtector for implementation within a SOX regulated environment. The standard and aggressive approaches are to be used as guidelines for setting the parameters of SafeGuard PortProtector and not to be interpreted as additional SOX requirements. In fact the SOX regulation does not specify protection requirements down to this level of detail. However, these configuration settings do follow general security principles and can be used as a baseline in creating a policy set for your own organization.

Setting	Standard SOX Approach	Aggressive SOX Approach	Rationale
Policy		Create new policies based on the built-in policy of Standard SOX or Aggressive SOX. Each policy can then be modified as determined by the SOXcompliance officer and in accordance with the organization's business objectives.	
Port Control:			
USB	Restrict	Restrict	Restricting access to these ports allows for a finer
FireWIre	Restrict	Restrict	

Setting	Standard SOX Approach	Aggressive SOX Approach	Rationale
PCMCIA	Restrict	Restrict	granularity of control under the device control section of the policy-security.
SD	Allow	Allow	Allowing access to these ports is required for some standard human interface devices. The access restrictions to these ports for storage devices will be further restricted through storage control below.
Serial	Allow	Allow	
Parallel	Allow	Allow	
WiFi	Restrict	Restrict	Restricting access to WiFi networks allows for a finer granularity of control under the WiFi control section of the policy-security.
Modem	Allow + log	Allow + log	Use of Modem, IrDA, or Bluetooth can lead to unauthorized network connections. At a minimum use of these ports should be logged. A more aggressive posture would block and log IrDA and Bluetooth links. Blocking user access to these links while connected to the TCP/IP network interface protects endpoints from the dangerous practice of hybrid network bridging.
IrDA	Allow + log	Block + log	
Bluetooth	Allow + log	Block + log	
Network Bridging	Block (All)	Block (All)	Blocking user access to WiFi, Bluetooth, Modems, and IrDA links while connected to the TCP/IP network interface protects endpoints from the dangerous practice of hybrid network bridging.
Device Control			
Hardware Keyloggers	Allow	Allow	Although the use of hardware keyloggers should be restricted and users should be protected from these attacks, usability concerns override the need for this restriction.

Setting	Standard SOX Approach	Aggressive SOX Approach	Rationale
Human Interface	Allow	Allow	It is typically not considered a risky practice to allow users to connect to human interface devices such as keyboards and mice.
Printers	Allow	Allow	Although a printer can be a data leakage source, printing is a common user function within most organizations. Compared to storage devices and PDAs, printers have a much lower capacity to "leak" large amounts of EPHI. This risk can be mitigated by physical and administrative controls.
PDA **Mobile Phones** **Imaging** **Audio / video Devices**	Restrict, White List, Log	Restrict, White List, Log	PDAs, mobile phones, Imaging devices (such as scanners) and Audio / Video devices (such as MP3 players) present a clear risk to the control and protection of data and networks. Organizations must ensure that any use of PDAs or Mobile phones supports encryption of sensitive information. Access to such devices should be restricted to an approved list of devices such as company issued PDAs and such access should be logged.
Network Adapters	Allow	Allow	Network adapters allow the PC to be connected to a network. This is a common configuration and should not be blocked or logged.
Smart Cards	Allow	Allow	Smart Cards are common as an authentication device. They do not pose a reasonable threat to the organization's assets.

Setting	Standard SOX Approach	Aggressive SOX Approach	Rationale
Content security devices	Allow	Allow	Content security devices monitor the content of the flow of data to and from the endpoint. If such devices are present they are part of a solution to enforce security and should not be blocked at the endpoint.
Unclassified devices	Block + Log	Block + Log	Unclassified devices are any devices that are not otherwise specified. These should not turn up very often. At a minimum there connection should be logged. An aggressive setting would block access to these devices.
Storage Control			
Autorun function	Block autorun function	Block autorun function	A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat and should be disabled by default.
Removable storage	Encrypt + log Block smart function	Encrypt + log Block smart function	Storage devices present a clear risk to the organization's assets. At a minimum a SOX organization restrict the use of storage devices to approved devices. Any data being written to storage devices should be encrypted; providing further protection in the event the storage device is lost or stolen.
External HD	Encrypt + log	Encrypt + log	
CD/DVD	Encrypt + log Block unsupported formats	Encrypt + log Block unsupported formats	
Floppy Drives	Read only + log	Read only + log	
Tape Drives	Restrict + log	Restrict + log	

Setting	Standard SOX Approach	Aggressive SOX Approach	Rationale
File Control	Allow + Log – write only	Allow + Log – write only	In order to support audit and investigation of security incidents involving EPHI log all files written to external storage devices.
WiFi Network	Allow + Log	Restrict , white list WPA encrypted networks, log	Wireless networks present a clear risk to the control and protection of data. At a minimum a SOX regulated organization should log any such behavior. However, the organization should use other internal controls to ensure that all wireless networks are secured through adequate encryption. A more aggressive setting to not only log the behavior but restrict use to an approved list of Wi-Fi networks that have been approved by the organization and have proper encryption.
P2P	Block + log	Block + log	
Policy Settings			
Logging	Send logs to SafeGuard PortProtector Server Send logs every 12 hours Log connect and disconnect events	Send logs to SafeGuard PortProtector Server Send logs every 12 hours Log connect and disconnect events	Logs should clearly not be stored on the endpoint, but instead sent to the SafeGuard PortProtector Server where they can be protected and viewed by the administrator. Other logging settings here provide adequate EPHI protection by ensuring periodic updating of logs on the server without burdening the network; inclusion of connect and disconnect events to allow for analysis of how long a device was connected;

Setting	Standard SOX Approach	Aggressive SOX Approach	Rationale
End-user messages	Review the end user messages associated with the SOX setting to ensure they are consistent with your formally documented security policies and security awareness training program.		It is important to provide a constant reminder to system users that they are responsible for protecting the network and sensitive information and complying with policies. Modifying the end-user messages to specifically mention SOX security will assist in the security awareness of your organization.
Encryption	Do not allow users to access encrypted devices at home Approve read only access for non-encrypted devices.	Do not allow users to access encrypted devices at home Approve read only access for non-encrypted devices.	It is important to restrict the use of EPHI to systems with adequate protection measures. Home computers generally lack HIPAA required security controls. Setting read-only for non-encrypted devices allows the flexibility of importing information without exposing EPHI to the risk of disclosure from loss or theft of a non-encrypted device.
Options	Use a different password from the client administration password to uninstall SafeGuard PortProtector Full visibility on endpoints	Use a different password to uninstall SafeGuard PortProtector Full visibility on endpoints	In order to enforce the principle of separation of duty and general password security, use a different password for the uninstall process of SafeGuard PortProtector Client than the client administration password. Consistent with the advice under “end user messages” it is best to let users know about the protections SafeGuard PortProtector is providing.

14.2.3 Other SafeGuard PortProtector SOX Settings

For the appropriate setting of other SafeGuard PortProtector features and options refer to the *Pre-Requisites for Addressing SOX Compliance Issues* detailed in this document. Specifically, the following SafeGuard PortProtector features should follow the business objectives and the sensitive data environment as defined in *Foundations*, *Considerations*, and *Preparations*.

Alerts

SafeGuard PortProtector alerts provide oversight of administrative actions and protection of the SafeGuard PortProtector security functions in case of attempted tampering. The following alert options should be set in order to preserve the security functions provided by SafeGuard PortProtector:

- Log all administrative eventsLogs all administrative actions and provides oversight of SafeGuard PortProtector administration.
- Alert all tempering eventsDetects tempering attempts and ensures the integrity of end point protection controls.

SafeGuard PortProtector Administration

SafeGuard PortProtector may be run by a single administrator or an organization may implement additional access control by defining additional administrators to a subset of administrative functions. This is an implementation of role-based access control and should be considered based on the organizations approach as defined in "Preparation 3: Determine Administrative Roles" which can be found under *Preparations* .Among the roles within the sensitive data environment the organization should consider are the following:

- Log Reviewer - Access to all logs and log functions without ability to edit policies.
- Policy Administrator - Access to edit and administer policies without ability to view logs.
- Audit - Read-only access to administrators console without ability to perform any changes.

The setting of these roles should be based on the administration model and approach of the organization and the support needed for incident response and maintenance. Refer to *Pre-Requisites for Addressing SOX Compliance Issues* for more complete instructions for SafeGuard PortProtector implementation preparation.

Domain Partitioning

Further access control granularity may be added with the SafeGuard PortProtector domain partitioning feature. The role based access mechanism includes domain partitioning, which allows an administrator role to be limited to a specific group of clients. This feature is useful in establishing the boundaries of the sensitive data environment by restricting the administrator's access within defined domains. The setting of these roles should be based on the organization's administration model and approach and the support needed for incident response and maintenance. Refer to *Pre-Requisites for Addressing SOX Compliance Issues* for more complete instructions for the SafeGuard PortProtector implementation preparation.

Administrative Password Strength

All passwords that protect system components within the sensitive data environment must comply with the organization's formally documented password policies. Formally documented security policies are discussed in more detail in "Consideration 1: Policies and Procedures" under *Considerations* section. Based on the organization's password strength policy, SafeGuard PortProtector administrative password strength criteria should be defined in the SafeGuard PortProtector to enforce organizational policies. Elements of the password strength include minimum length and required character types.

14.2.4 Relevant SOX Requirements

SOX Requirement		
P04.6	Roles and responsibilities	Roles and responsibilities must be defined and communicated throughout the organization. Once create, these roles must be maintained.
P04.8	Responsibility for risk, security	Specific roles must be created for critical tasks that involve risk management for information security and compliance.
P04.9	Data and system ownership	Owner for critical information must be defined and provided with systems that enforce the data classification.
P06.2	Enterprise IT risk and internal	The IT framework should deliver a minimal risk at a high value (low cost). Reduction of risks should include preventative, detective and corrective measures to protect business assets.
PO7.8	Job change and termination	In the case of a job change, access rights should be redefined such that risks are minimized.
PO9.3	Event identification	Any potential threats to the infrastructure should be identified, together with the potential impact.
DS5.4	User account management	Any IT implementation must contain a logging and monitoring function that provides early detection of unauthorized activities.
DS5.6	Security incident definition	Security incidents must be clearly defined to ensure that the response follows the incident response process.
DS5.7	Protection of security technology	All security related functions must be tamper resistant such that they cannot be bypassed by unauthorized access.
DS5.10	Network security	Information flows to and from networks must be controlled with security techniques and related management procedures.
ME2.1	Monitoring of Internal	The IT environment and controls must be

	Control Framework	continuously monitored.
AC18	Protection of sensitive information during transmission and transport	Controls must be deployed to protect the confidentiality and integrity of sensitive information during transmission and transport.

15 Appendix G – Using SafeGuard PortProtector in a PCI Regulated Organization

About This Appendix

In order to create protection of cardholder data credit card companies such as VISA International, MasterCard Worldwide, Discover Financial Services, American Express, and JCB issued security compliance requirements to merchants that processed, stored, or transmitted cardholder information. Although each of these security programs was issued by their respective organizations, the programs were similar in terms of protection requirements. In 2004 the Payment Card Industry (PCI) Security Standards Council was formed to create a common set of requirements for credit card processing merchants. The PCI Data Security Standard (DSS) v1.1 contains the current set of requirements for credit card merchants.

Specifically the PCI DSS control objectives ensure that the organization builds and maintains a secure network; protects cardholder data; maintains a vulnerability management program, implements strong access control measures, monitors and tests networks, and maintains an information security policy. Ensuring security at the endpoints within a network that processes cardholder data is one of the issues that must be addressed by PCI organizations.

SafeGuard PortProtector helps you regain control of your endpoints and address data leakage and targeted attack threats. This chapter provides guidance on how to address these threats within a PCI DSS regulated environment.

The first section, *Pre-Requisites for Addressing PCI DSS Compliance Issues*, examines organizational issues and pre-requisites that must be addressed prior to implementing SafeGuard PortProtector security features and settings. It contains the following sub-sections:

- *Foundations* translates business objectives into a PCI DSS compliant context.
- *Considerations* describes the information security threats that must be addressed within the context of the established business mission.
- *Preparations* describes the activities that should be performed before configuring SafeGuard PortProtector for protection

The second section, *SafeGuard PortProtector PCI DSS Settings* section provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product. It contains the following sub-sections:

- *PCI DSS Policy Settings* describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a PCI DSS environment.
- *Other* SafeGuard PortProtector *PCI DSS Settings* describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to the business objectives and the environment of the PCI organization.
- *PCI DSS* / SafeGuard PortProtector *Feature Mapping* provides additional advice on how SafeGuard PortProtector helps to meet PCI DSS Security Rule requirements.

15.1 Pre-Requisites for Addressing PCI DSS Compliance Issues

SafeGuard PortProtector provides many security features that can address the threats of endpoint security. In order to effectively utilize the capabilities of the product, the PCI DSS regulated organization should take some preliminary actions to must prepare to use SafeGuard PortProtector for PCI DSS compliance.

There are three categories of pre-requisites for effective implementation of SafeGuard PortProtector for PCI DSS compliance. The first category is *Foundations*. Foundations are basic information security program elements that must be in place in order for any compliance effort to move forward. Foundations include the establishment of business mission statements, and roles, responsibilities required to carry them out. The second pre-requisite is *Considerations*. Considerations are specific information security threats that must be addressed within the context of the established business mission. In this case considerations are specific issues regarding the protection of stored cardholder data in light of endpoint security. The third pre-requisite for effective implementation is *Preparations*. Preparations are activities that must be performed prior to installing and configuring a specific technology product such as SafeGuard PortProtector.

15.1.1 Foundations

The evaluation of security controls within an organization requires a context of business objectives. For PCI DSS regulated organizations that context is provided by the following set of foundations that translate business objectives into a PCI DSS compliant context for the implementation of technology.

Foundation 1: Information Security Program

An information security program consists of dedicated security professionals supported by management with the appropriate scope, authority, and budget to assess information security risks, recommend mitigation techniques and ensure appropriate security risk management of the organization's assets. A strong information security program will include an identification of reasonable threats to the organization's assets, a review of the physical, administrative, and technical controls, and the planning and implementation oversight of security controls to bring the security posture to an acceptable assurance level. Any organization responsible for the protection of cardholder data will need a strong baseline of security controls and organizational support to implement PCI DSS requirements.

Foundation 2: PCI Compliance Project

Demonstrating compliance with PCI DSS requirements will require internal and external resources sufficient to manage the project, assess current controls, create or revise existing security policies and procedures, and configure or install new information technology. This compliance process will require resources with experience in your organization's business objectives and current technology infrastructure as well as resources with experience in PCI DSS compliance readiness or assessment. The compliance process can be a demanding one. Recognizing the resource requirements is the first step.

15.1.2 Considerations

To enforce the security cardholder data, there are twelve security control objectives that must be met, each with a set of requirements implementing the objective. Prior to embarking on an effort to implement each requirement a PCI DSS organization should first consider several key elements of the upcoming PCI DSS compliance project. Careful consideration of these elements can help an organization avoid several common pitfalls and increase its efficiency in the PCI DSS compliance effort.

Consideration 1: Data Architecture

The root of the PCI DSS requirements is the protection of cardholder data and sensitive authentication data. Cardholder data includes the Primary Account Number (PAN), the cardholder's name, the service code, and the expiration date of the card. Sensitive authentication data includes the information on the "full magnetic stripe", the security code (e.g. CVC2), and the PIN for the card. Sensitive authentication data is protected by ensuring that it is never stored. Cardholder data is required to be protected if it is stored, processed, or transmitted within your organization's applications or systems.

Data architecture is the logical arrangement and association of data elements throughout your system. The structure of your data architecture dictates the application of the PCI DSS requirements on your organization. For example, if your network does not distinguish between cardholder data environments and the rest of your network then it could be argued that the entire network is under the PCI DSS requirements. On the other hand, if you have adequate policies and procedures (such as data classification policies), adequate network separation, and well defined cardholder data applications, then you could argue that only portions of your network fall under the PCI DSS requirements.

Consideration 2: Data Environment Separation

The PCI DSS requirements apply to all elements of your cardholder data environment. This includes components of the systems such as network components (e.g. switches, routers firewalls, wireless access points, network appliances, and security appliances), servers (e.g. mail servers, proxy servers, web servers, authentication servers, database servers, domain name servers), and applications (custom or commercial, internal or external facing). System components that are properly separated from the cardholder data environment are not required to meet the PCI DSS requirements. Proper network segmentation and other means of data environment separation can establish a proper environment to protect cardholder data and reduce the overall work required to become PCI DSS compliant. Endpoints within cardholder data network segments would need appropriate protection as defined under PCI DSS and detailed in this document.

Consideration 3: Policies and Procedures

A security policy is a statement of management's intent for protecting corporate assets from fraud, waste, and abuse. To be compliant with PCI DSS, the organization must have a strong security policy that provides the employees with security awareness and informs them of their responsibilities for protecting the organization's assets. Specifically, PCI DSS requires a security policy address the following relevant areas concerning the implementation of a technology such as SafeGuard PortProtector:

- Technology Usage Policy. A PCI organization is required to have a usage policy for "employee-facing" technology. The organization will require management approval of the SafeGuard PortProtector product and an update to the acceptable use policies regarding the administration of SafeGuard PortProtector.
- Information Security Responsibilities. A PCI organization is required to define and assign information security and security management responsibilities for all employees and contractors. The organization will need to update job descriptions (or other means of assigning security responsibilities) to include the administration of the SafeGuard PortProtector product.
- Formal Awareness Program. A PCI organization is required to implement a formal security awareness program. The introduction of SafeGuard PortProtector to endpoints (i.e. desktops and laptops) will require an update to the user education.

15.1.3 Preparations

SafeGuard PortProtector allows organizations to control access and protect endpoints based on user roles, network domains, computer types, and systems and data sensitivity. The specific implementation and configuration of SafeGuard PortProtector requires an accurate knowledge of objects SafeGuard PortProtector is to protect, the policies it is to enforce, and the administrative roles that will maintain the SafeGuard PortProtector software. The following activities are an important element of the preparation to install and configure SafeGuard PortProtector for the protection of cardholder data.

Preparation 1: Determine Endpoint Protection Needs

SafeGuard PortProtector provides the ability to protect stored cardholder data for uncontrolled export on removable devices at endpoints. On the other hand your organization has a variety of business needs that will require connectivity to external storage devices, wireless networks, and other possible threats. In preparation for a SafeGuard PortProtector deployment your organization should determine the protection and business needs of the endpoints.

Instructions:

- Update endpoint inventory and classification. Be sure that you are aware of all endpoints within your network that store, process, or transmit cardholder data. This can be done through a manual inventory process of through the use of directory services. Classification is based on your data classification policy and includes a classification of endpoints that handle cardholder data.
- Scan each endpoint to detect port, device, and Wi-Fi usage. The SafeGuard PortAuditor utility will automatically detect devices and networks that are currently or previously connected.

- Review your security policies and procedures, specifically as they address security design principles such as "Default – No Access" and "Least Privilege". These policies and procedures should be applied to the endpoints that have now been inventoried, classified, and scanned. Make a list of the intended profiles for each endpoint classification.

Preparation 2: Determine User Access Roles

SafeGuard PortProtector allows for the specification of allowed ports, devices, and Wi-Fi usage according to user, user group, or organizational unit as defined by Active Directory or Novel eDirectory. It is important to note that any user privileges granted through this mechanism will trump those specified for an individual endpoint. For example, if you set up a user to have Wi-Fi access (over WPA networks) and have also locked down a laptop to block Wi-Fi access, that user will be able to gain Wi-Fi access through that laptop. With this rule in mind it is strongly recommended that you be very careful when creating any user privileges as those privileges will apply to any endpoint to into which that user logs.

Instructions:

- Determine user roles within your SafeGuard PortProtector implementation.
    - User – this role is the normal user role that has no additional privileges associated.
    - Privileged user – this role has extended privileges such as the use of a specifically permitted non-encrypting device.
- Determine compensating controls placed on privileged users.
- Logs and alerts – at a minimum plan to set privilege user policies to log allowed behavior that is extended from the normal user role. Consider setting alerts on highly sensitive behavior such as the use of a specifically permitted non-encrypting device.

Preparation 3: Determine Administration Roles

SafeGuard PortProtector allows for multiple administration roles according to privilege and domain. The use of these administrative role options should be determined prior to installation of SafeGuard PortProtector.

Instructions:

- Determine if your implementation of SafeGuard PortProtector will follow a centralized or de-centralized administration model.
- Centralized – a single entity is responsible for the administration of SafeGuard PortProtector .
- De-centralized – administration of SafeGuard PortProtector is delegated to departments that are responsible for the administration of their own domain. If you chose this method of administration, then determine the domain partitions for which each department will be responsible for the administration.
- Determine administration roles within each domain.
- The SafeGuard PortProtector administrator may be set up as a single role or you may delegate administrative privileges to implement separation of duties. Determine the set of administrative roles that you will implement.
- Plan maintenance and incident response function for SafeGuard PortProtector administration.

- Incident response – those responsible for responding to incidents involving lost or stolen storage devices, rogue networks, hybrid network bridging, or unapproved data removal will require special permissions within SafeGuard PortProtector and access to audit tools. Document the incident response roles within your organization and the permissions and access required.
- Maintenance – those responsible for handling end user issues such as peripherals and network connectivity will require the ability to request modifications to object or user permissions. Document maintenance roles within your organization and the permissions and access required.

15.2 SafeGuard PortProtector PCI DSS Settings

This section provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product.

- *PCI DSS Policy Settings* describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a PCI DSS environment.
- *Other SafeGuard PortProtector PCI DSS Settings* describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to the business objectives and the environment of the PCI organization.
- *PCI DSS / SafeGuard PortProtector Feature Mapping* provides additional advice on how SafeGuard PortProtector helps to meet PCI DSS Security Rule requirements.

15.2.1 PCI DSS Policy Settings

The following table is a guide to the SafeGuard PortProtector administrator in the setting and configuration of SafeGuard PortProtector for implementation within a cardholder data environment. Many of the settings below are a direct implementation of a specific PCI DSS requirement, while others follow good security practices consistent with the level of security achieved through the other PCI DSS requirements. The PCI DSS settings are to be used as guidelines for setting the parameters of SafeGuard PortProtector and not to be interpreted as additional PCI DSS requirements.

Setting	PCI Setting	Rationale
Policy		Create new policies based on the built-in policy of PCI DSS. Each policy can then be modified as determined by the compliance officer and in accordance with the organization's business objectives.
Port Control:		
USB	Restrict	Restricting access to these ports allows for a finer granularity of control under the device control section of the policy-security.
FireWire	Restrict	
PCMCIA	Restrict	
SD	Allow	Allowing access to these ports is required for some standard human interface devices. The
Serial	Allow	

Setting	PCI Setting	Rationale
Parallel	Allow	access restrictions to these ports for storage devices will be further restricted through storage control below.
WiFi	Restrict	Restricting access to Wi-Fi networks allows for a finer granularity of control under the Wi-Fi control section of the policy-security.
Modem	Allow + log	Use of Modem can lead to unauthorized network connections but may be a common business use. At a minimum use of these devices should be logged. Use of IrDA or Bluetooth can lead to unauthorized network connections. Use of these devices should be blocked and logged. Blocking user access to Wi-Fi, Bluetooth, Modems, and IrDA links while connected to the TCP/IP network interface protects endpoints from the dangerous practice of hybrid network bridging.
IrDA	Block + log	
Bluetooth	Block + log	
Network Bridging	Block (All)	
Device Control		
Hardware Keyloggers	Allow	Although the use of hardware keyloggers should be restricted and users should be protected from these attacks, usability concerns override the need for this restriction.
Human Interface	Allow	It is typically not considered a risky practice to allow users to connect to human interface devices such as keyboards and mice
Printers	Allow + log	Although a printer can be a data leakage source, printing is a common user function within most organizations. This risk can be mitigated by physical and administrative controls.
PDA	Restrict, white list, log	PDAs, mobile phones, Imaging devices (such as scanners) and Audio / Video devices (such as MP3 players) present a clear risk to the control and protection of cardholder data. The use of such devices should be blocked.
Mobile Phones		
Imaging		
Audio / video Devices		
Network Adapters	Allow	Network adapters allow the PC to be connected to a network. This is a common configuration and should not be blocked or logged.
Smart Cards	Allow	Smart Cards are common as an authentication device. They do not pose a reasonable threat to cardholder data.
Content security	Allow	Content security devices monitor the content of

Setting	PCI Setting	Rationale
devices		the flow of data to and from the endpoint. If such devices are present they are part of a solution to enforce security and should not be blocked at the endpoint.
Unclassified devices	Block + Log	Unclassified devices are any devices that are not otherwise specified. These should not turn up very often, and present a clear risk to the protection of cardholder data.
Storage Control		
Autorun function	Block	A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat and should be disabled by default.
Removable storage	Encrypt + log block smart function	Storage devices (such as USB drives) present a clear risk to the protection of cardholder data. The organization should limit the use of storage devices to approved devices with the ability to appropriately encrypt the data. Use of these devices should be logged. A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat and should be disabled by default. Certain formats for writing files to media such as CD or DVD do not support the event logging. To preserve the logging settings for all files the "block unsupported burning formats" option should remain checked.
External HD	Encrypt + log	
CD/DVD	Encrypt + log block unsupported burning formats	
Floppy Drives	Read only + log	
Tape Drives	Block + log	
File Control	Log – write only	In order to support audit and investigation of security incidents involving cardholder data, the organization should log all files written to external storage devices.
WiFi Network	Restrict, white list WPA encrypted networks, log	Wireless networks present a clear risk to the control and protection of cardholder data. At a minimum an organization should log any such behavior. Any use of Wi-Fi networks should be logged and limited to an approved list of Wi-Fi networks with proper encryption.
P2P	Block + log	

Setting	PCI Setting	Rationale
Policy Settings		
Logging	Send logs to SafeGuard PortProtector Server Send logs every 12 hours Log connect and disconnect events	Logs should clearly not be stored on the endpoint, but instead sent to the SafeGuard PortProtector Server where they can be protected and viewed by the administrator. Other logging settings here provide adequate cardholder protection by ensuring periodic updating of logs on the server without burdening the network; inclusion of connect and disconnect events to allow for analysis of how long a device was connected.
End-user messages	Review the end user messages associated with the PCI setting to ensure they are consistent with your formally documented security policies and security awareness training program.	It is important to provide a constant reminder to those exposed to cardholder data that they are responsible for protecting cardholder data and complying with policies. Modifying the end-user messages to specifically mention PCI security and cardholder data protection will assist in the security awareness of your organization.
Encryption	Do not allow users to access encrypted devices at home Approve read only access for non-encrypted devices	It is important to restrict the use of cardholder to systems with adequate protection measures. Home computers would generally fall outside of the cardholder data environment and should not have the ability to read cardholder data. Setting read-only for non-encrypted devices allows the flexibility of importing information without exposing cardholder data to the risk of disclosure from loss or theft of a non-encrypted device.
Options	Use a different password to uninstall SafeGuard PortProtector Full visibility on endpoints	In order to enforce the principle of separation of duty and general password security, use a different password for the uninstall process of SafeGuard PortProtector Client than the client administration password. Consistent with the advice under “end user messages” it is best to let users know about the protections SafeGuard PortProtector is providing to PCI security.

15.2.2 Other SafeGuard PortProtector PCI DSS Settings

For the appropriate setting of other SafeGuard PortProtector features and options refer to the *Pre-Requisites for Addressing PCI DSS Compliance Issues* detailed in part 1 of the PCI DSS Compliance with SafeGuard PortProtector document. Specifically, the following SafeGuard PortProtector features should follow the business objectives and the cardholder data environment as defined in *Foundations*, *Considerations*, and *Preparations*.

Alerts

SafeGuard PortProtector alerts provide oversight of administrative actions and protection of the SafeGuard PortProtector security functions in case of attempted tampering. The following alert options should be set in order to preserve the security functions provided by SafeGuard PortProtector :

- Log all administrative events - Logs all administrative actions and provides oversight of SafeGuard PortProtector administration.
- Alert all tempering events - Detects tempering attempts and ensures the integrity of end point protection controls.

SafeGuard PortProtector Administration

SafeGuard PortProtector may be run by a single administrator or an organization may implement additional access control by defining additional administrators to a subset of administrative functions. This is an implementation of role-based access control and should be considered based on the organizations approach as defined in "Preparation 3: Determine Administrative Roles" under *Preparations* section. Among the roles within the cardholder data environment the organization should consider are the following:

- Log Reviewer -Access to all logs and log functions without ability to edit policies.
- Policy Administrator - Access to edit and administer policies without ability to view logs.
- Audit - Read-only access to administrators console without ability to perform any changes.

The setting of these roles should be based on the administration model and approach of the organization and the support needed for incident response and maintenance. Refer to *Pre-Requisites for Addressing PCI DSS Compliance Issues* for more complete instructions for SafeGuard PortProtector implementation preparation.

Domain Partitioning

Further access control granularity may be added with the SafeGuard PortProtector domain partitioning feature. The role based access mechanism includes domain partitioning, which allows an administrator role to be limited to a specific group of clients. This feature is useful in establishing the boundaries of the cardholder data environment by restricting the administrator's access within defined domains. The setting of these roles should be based on the organization's administration model and approach and the support needed for incident response and maintenance. Refer to *Pre-Requisites for Addressing PCI DSS Compliance Issues* for more complete instructions for the SafeGuard PortProtector implementation preparation.

Administrative Password Strength

All passwords that protect system components within the cardholder data environment must comply with the organization's formally documented password policies and PCI DSS requirement 8.5. Formally documented security policies are discussed in more detail in "Consideration 1: Policies and Procedures" under *Considerations* section. Required elements of the password strength include a minimum length of seven (7) characters, at least one (1) character, and at least one (1) number.

15.2.3 PCI DSS / SafeGuard PortProtector Feature Mapping

SafeGuard PortProtector provides PCI DSS organizations additional technical controls to protect cardholder data at system endpoints and address data leakage and targeted attack threats. As discussed throughout this document SafeGuard PortProtector can address data leakage risks, targeted attack threats, and many of the PCI DSS requirements. Although obvious, it should be noted that SafeGuard PortProtector provides a portion of the control objectives necessary for complete PCI DSS compliance. The table below provides additional advice on how SafeGuard PortProtector helps to meet PCI DSS requirements.

<table>
<tr><td colspan="4"><u>PCI</u></td></tr>
<tr><td>Requirement Number</td><td>Requirement Description</td><td>Relevant SafeGuard PortProtector Features</td><td>How to Satisfy PCI DSS Controls with SafeGuard PortProtector</td></tr>
<tr><td>2</td><td>Do not use vendor-supplied defaults for system passwords and other security parameters.</td><td rowspan="2">SafeGuard PortProtector provides administrators the ability to change passwords (including the default password).</td><td rowspan="2">Change the default administration and install passwords for SafeGuard PortProtector.</td></tr>
<tr><td>2.1</td><td>Always change vendor-supplied defaults before installing a system on the network.</td></tr>
<tr><td>2.2.2</td><td>Disable all unnecessary and insecure services and protocols….</td><td rowspan="2">SafeGuard PortProtector provides the ability to block access to unnecessary ports and storage devices that may pose a threat to cardholder data.</td><td rowspan="2">Use the SafeGuard PortProtector recommended settings for port, device, storage, file, and Wi-Fi network control to block or restrict access to unnecessary devices. [See recommended settings in table above.]</td></tr>
<tr><td>2.2.4</td><td>Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.</td></tr>
</table>

4.1.1	For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi protected access (WPA or WPA2) technology…..	SafeGuard PortProtector allows the organization to create policies that force the use of encrypted Wi-Fi channels for secure transfer of data. These policies can even be set to require a specific level of encrypted (e.g. WPA).	Under port control, restrict Wi-Fi networks. Under Wi-Fi networks set a white list of approved Wi-Fi networks to WPA encrypted networks.
8	Assign a unique ID to each person with computer access	SafeGuard PortProtector provides the ability to unique user IDs for all administrative users.	For all SafeGuard PortProtector administrative accounts assign a single account to a single user – no group administration accounts. Set password complexity to a minimum of seven (7) characters and at least one number and at least one letter.
8.1	Identify all users with a unique user name before allowing them to access system components or cardholder data.		
8.2	In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: (Password, Token devices, Biometrics)		
9	Restrict physical access to cardholder data	SafeGuard PortProtector can be applied to network endpoints to restrict data leakage or unintended data transfers between systems. PCI organizations must limit system components that require access, transmission, or storage of cardholder data and physically separate these from other network components.	See “Consideration 2: Data Environment Separation” for a discussion of separating the cardholder data environment.

10	Track and monitor all access to network resources and cardholder data	SafeGuard PortProtector records endpoint events associated with storage devices and media in client logs. An event may be a device connection or disconnection, a wireless network connection, tampering attempts or administrator login. Event logs include endpoint identify, user, event type, and time. SafeGuard PortProtector also creates server logs for administrative events such as administrator login, publishing policies and performing backups.	Use the SafeGuard PortProtector recommended logging settings for port, device, storage, file, and Wi-Fi network control to block or restrict access to unnecessary devices. [See recommended settings in table above.] Log all administrative events and alert to all tempering events.
10.2	Implement automated audit trails for all system components to reconstruct the following events: Individual user accesses to cardholder data All actions taken by any individual with administrative privileges Access to all audit trials Invalid logical access attempts Use of identification and authentication mechanisms Initialization of the audit logs.		
10.3	Record at least the following audit trail entries for all system components for each event: User identification Type of event Data and time Success or failure indication Origin of event Identity or name of affected data, system component, or resource.		
10.4	Synchronize all critical system clocks and times	SafeGuard PortProtector audit log timestamps are based on the system time of the endpoint.	Audit log timestamps are a built-in function of SafeGuard PortProtector. To synch system clocks, apply controls such as network time protocol to the desktop.

10.5	Secure audit trails so they cannot be altered.	Client and Server logs are sent to a log repository and stored on the Management Server at the defined intervals.	Use the SafeGuard PortProtector recommended settings for logging:
12	Maintain a policy that addresses information security for employees and contractors.	SafeGuard PortProtector is a technology control that can implement policies and procedures to prevent and detect security violations at the network endpoints.	See consideration 3 [Policies and Procedures] for instructions on what policies and procedures need to be implemented.

16 Appendix H – Using SafeGuard PortProtector in a FISMA Regulated Organization

About This Appendix

The E-Government Act (Public Law 107-347) passed by the 107th US Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

SafeGuard PortProtector helps you control your endpoints and address data leakage and targeted attack threats. This chapter provides guidance on how to address these threats within a FISMA-regulated environment.

The first section Pre-Requisites for Addressing FISMA Compliance Issues, examines organizational issues and pre-requisites that must be addressed prior to implementing SafeGuard security features and settings. It contains the following sub-sections:

- Foundations translates operational objectives into a FISMA compliant context.
- Considerations describes the information security threats that must be addressed within the context of the established mission requirements.
- Preparations describes the activities that should be performed before configuring SafeGuard for protection.

The second section, Implementing SafeGuard PortProtector in a FISMA Regulated Organization, provides specific Sophos setting guidance for the policy, user, and administrator parameters within the Sophos solution. It contains the following sub-sections:

- FISMA policy settings describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a FISMA environment.
- Other SafeGuard FISMA Settings describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy according to operational objectives and the environment of the FISMA organization.
- FISMA/SafeGuard PortProtector Feature Mapping provides additional advice on how SafeGuard PortProtector helps to meet FISMA Security Rule requirements.

16.1 Pre-Requisites for Addressing FISMA Compliance Issues

SafeGuard PortProtector provides many security features that can address the threats of endpoint security. In order to effectively utilize the capabilities of the product, the FISMA regulated organization should take some preliminary actions to prepare to use SafeGuard PortProtector for FISMA 404 compliance.

There are three categories of pre-requisites for effective implementation of SafeGuard PortProtector for FISMA compliance. The first category is Foundations. Foundations are basic information security program elements that must be in place in order for any compliance effort to move forward. Foundations include the establishment of mission statements, and roles, responsibilities required to carry them out. The second pre-requisite is Considerations. Considerations are specific information security threats that must be addressed within the context of the established objectives. The third pre-requisite for effective implementation is Preparations. Preparations are activities that must be performed prior to installing and configuring a specific technology product such as SafeGuard PortProtector.

16.1.1 Foundations

The evaluation of security controls within an organization requires a context of operational objectives. For FISMA regulated organizations that context is provided by the following set of foundations that translate mission objectives into a FISMA compliant context for the implementation of technology.

Foundation 1: Information Security Program

An information security program consists of dedicated security professionals supported by management with the appropriate scope, authority, and budget to assess information security risks, recommend mitigation techniques and ensure appropriate security risk management of the organization's assets. A strong information security program will include an identification of reasonable threats to the organization's assets, a review of the physical, administrative, and technical controls, and the planning and implementation oversight of security controls to bring the security posture to an acceptable assurance level.

Foundation 2: FISMA Compliance Project

Demonstrating compliance with FISMA baseline requirements will require internal and external resources sufficient to manage the project, assess current controls, create or revise existing security policies and procedures, and configure or install new information technology. This compliance process will require resources with experience in your organization's mission objectives and current technology infrastructure as well as resources with experience in FISMA compliance readiness or assessment. The compliance process can be a demanding one. Recognizing the resource requirements is the first step.

16.1.2 Considerations

To ensure the protection of the organization's assets there are a number of control objectives that must be met. Prior to embarking on an effort to implement these control objectives, the FISMA organization should first consider several key elements of the upcoming FISMA compliance project. Careful consideration of these elements can help an organization avoid several common pitfalls and increase its efficiency in the FISMA compliance effort.

Consideration 1: Risk Assessment

The basic step of any information security policy is to determine which information needs to be protected, and which personnel, systems and devices may or may not be granted access to it. A comprehensive risk assessment plan should be based upon, or include a detailed review and categorization of confidential information in the organization according to risk levels. Based on outcome of the risk assessment procedure, it will be possible to determine the proper security controls needed to protect confidential information and information systems.

Instructions:

- Review the threats facing information systems in the organization, and the channels through which information might leak out of the organization. Assess the potential damage and harm that may result from unauthorized access, disclosure, or loss of such information.
- Create an inventory of all peripheral devices used by your organization, and specifically of all storage and storage-enabled device (such as smart phones, media players, etc).
- Determine which systems, personnel, and peripheral devices may access confidential information, and how they may be used inside and outside of the organization.

Consideration 2: Policies and Procedures

A security policy is a statement of management's intent for protecting corporate assets from fraud, waste, and abuse. With the emergence of the data leakage threat data access policies and procedures must be reviewed and revised. The principle of least privilege, which states that each user should have only the level of access required to perform their job, needs to be interpreted to address portable media and devices.

Instructions:

- Ensure that your current policies are based on the principle of "Default – No Access". This principle dictates that by default all users have no access to any corporate resources. If no such policy statement exists – create one.
- Develop a guidance policy that interprets the "Default – No Access" policy for the roles within your organization and to the computing devices within your organization.
- Develop procedures for handling exceptions to the "Default – No Access" policy. These exceptions will be based on operational needs such as media backup, data transfer, and remote access to networks for telecommuting. Each procedure should address the risk through compensating controls such as policy, sanctions, asset tracking, multi-factor authentication, oversight, and encryption.

Consideration 3: Training

Effective security awareness and training is an important element of asset protection. Information security training programs need to be periodically updated to reflect changes in threats and organizational policies. A project to update security awareness and training programs should be part of the overall data leakage risk mitigation project.

Instructions:

Update annual security awareness training and periodic security awareness reminders to include a discussion of data leakage threats, updated policies, required user actions, prohibited behavior, and restricted devices.

- Wi-Fi Threats: use on unapproved networks, rogue networks, hybrid network bridging, WEP authentication.
- Mobile/Storage Device Threats: physical loss, data removal, malicious code insertion.

Consideration 4: Incident Response

In the event of a security breach resulting in the disclosure, modification, or interruption of service, FISMA compliant organizations are required to have policies, procedures, and the capability of investigating the incident. As the set of possible security incidents expands to include data leakage, organizations must update their policies, procedures, and capabilities to respond to these incidents.

Instructions:

Update the incident response procedures to address data leakage issues. Specifically, create procedures for the following incident types.

- Lost or stolen mobile/storage device
- Found rogue network
- Found hybrid network bridging
- Unapproved data removal

16.1.3 Preparations

SafeGuard PortProtector enables organizations to control access and protect endpoints based on user roles, network domains, computer types, and criticality of systems and data. The specific implementation and configuration of SafeGuard PortProtector requires an accurate knowledge of the objects SafeGuard PortProtector is to protect, the policies it is to enforce, and the administrative roles that will be used to maintain the SafeGuard PortProtectorsoftware. The following activities are an important part of the preparation to install and configure SafeGuard PortProtector for the implementation of appropriate internal controls.

Preparation 1: Determine Endpoint Protection Needs

SafeGuard PortProtector provides the ability to protect stored data for uncontrolled export on removable devices at endpoints. On the other hand your organization has a variety of operational needs that will require connectivity to external storage devices, wireless networks, and other possible threats. In preparation for a SafeGuard PortProtector deployment your organization should determine the protection and operational needs of the endpoints.

Instructions:

- Update endpoint inventory and classification. Be sure that you are aware of all the endpoints within your network that store, process, or transmit sensitive data. This can be done through a manual inventory process or through the use of directory services. Classification is based on your data classification policy and includes a classification of endpoints that handle sensitive data.
- Scan each endpoint to detect port, device, and Wi-Fi usage. The SafeGuard Auditor utility will automatically detect devices and networks that are currently or previously connected.
- Review your “Default – No Access” and least privilege policies, as they apply to the endpoints that have now been inventoried, classified, and scanned. Make a list of the intended profiles for each endpoint classification.

Preparation 2: Determine User Access Roles

SafeGuard PortProtector allows specifing the allowed ports, devices, and Wi-Fi usage according to user, user group, or organizational unit as defined by Active Directory or Novel eDirectory. It is important to note that any user privileges granted through this mechanism will trump those specified for an individual endpoint. For example, if you set up a user to have Wi-Fi access (over WPA networks) and also have locked down a laptop to block Wi-Fi access, that user will be able to gain Wi-Fi access through that laptop. With this rule in mind it is strongly recommended that you be very careful when creating any user privileges, since these privileges will apply to any endpoint into which that user logs.

Instructions:

- Determine user roles within your SafeGuard PortProtector implementation.
- User – this role is the normal user role that has no additional privileges associated.
- Privileged user – this role has extended privileges such as the ability to write files to a USB device or connect to a WPA-enabled Wi-Fi network.
- Determine compensating controls placed on privileged users.
- Logs and alerts – at the minimum, plan to set privileged user policies to log allowed behavior that is extended from the normal user role. Consider setting alerts on highly sensitive behavior such as connecting to external hard drives.

Preparation 3: Determine Administration Roles

SafeGuard PortProtector allows for multiple administration roles according to privilege and domain. The use of these administrative role options should be determined prior to installation of SafeGuard PortProtector.

Instructions:

- Determine if your implementation of SafeGuard PortProtector will follow a centralized or de-centralized administration model.
- Centralized – a single entity is responsible for the administration of SafeGuard PortProtector.
- De-centralized – administration of SafeGuard PortProtector is delegated to departments that are responsible for the administration of their own domain. If you chose this method of administration, then determine the domain partitions for each department which will be responsible for the administration.
- Determine administration roles within each domain.
- The SafeGuard PortProtector administrator may be set up as a single role or you may delegate administrative privileges to implement separation of duties. Determine the set of administrative roles that you will implement.
- Plan maintenance and incident response function for SafeGuard PortProtector administration.
- Incident response – those responsible for responding to incidents involving lost or stolen storage devices, rogue networks, hybrid network bridging, or unapproved data removal will require special permissions within SafeGuard PortProtector and access to auditing tools. Document the incident response roles within your organization and the permissions and access required.
- Maintenance – those responsible for handling end user issues such as peripherals and network connectivity will require the ability to request modifications to object or user permissions. Document maintenance roles within your organization and the permissions and access required.

16.2 Implementing SafeGuard PortProtector in a FISMA Regulated Organization

This section provides specific SafeGuard PortProtector setting guidance for the policy, user, and administrator parameters within the SafeGuard PortProtector product.

- FISMA policy settings, describes the setting and configuration of SafeGuard PortProtector Policies for implementation within a FISMA regulated environment.
- Other SafeGuard PortProtector FISMA Settings, describes the setting and configuration of SafeGuard PortProtector Settings that are not a part of the policy.
- FISMA/SafeGuard PortProtector Feature Mapping, provides additional information on the FISMA Security Rule requirements.

16.2.1 FISMA policy settings

The following table is a guide for the SafeGuard PortProtector administrator in the setting and configuration of SafeGuard PortProtector for implementation within a FISMA regulated environment. SafeGuard PortProtector provides organizations with additional technical controls to protect cardholder data at system endpoints and address data leakage and targeted attack threats. As discussed throughout this appendix, SafeGuard PortProtector can address data leakage risks, targeted attack threats, and many of the FISMA requirements.

Setting	FISMA Setting	Rationale
Policy		Create new policies based on the built-in policy of FISMA best practices. Each policy can then be modified as determined by the compliance officer and in accordance with the organization's operational needs.
Port Control:		
USB	Restrict	Restricting access to these ports allows for a finer granularity of control under the device control section of the policy-security.
FireWire	Restrict	
PCMCIA	Restrict	
SD	Allow	Any storage-capable devices connected to this port will be allowed or blocked based on the permissions defined by storage device settings.
Serial	Allow	Allowing access to these ports is required for some standard human interface devices.
Parallel	Allow	
WiFi	Restrict	Restricting access to Wi-Fi networks allows for a finer granularity of control under the Wi-Fi control section of the policy-security.
Modem	Allow + log	Use of a modem can lead to unauthorized network connections but may have a common business use. At the minimum, however, use of these devices should be logged.
IrDA	Block + log	Use of IrDA or Bluetooth can lead to unauthorized network connections. Use of these devices should be blocked and logged.
Bluetooth	Block + log	
Network Bridging	Block (All)	Blocking user access to Wi-Fi, Bluetooth, modems, and IrDA links while connected to the TCP/IP network interface, protects endpoints from the dangerous practice of hybrid network bridging.
Device Control:		
Hardware Keyloggers	Allow	Although the use of hardware keyloggers should be restricted and users should be protected from these attacks, usability concerns override the need for this restriction.
Human Interface	Allow	It is typically not considered risky to allow users to connect to human interface devices, such as keyboards and mice.
Printers	Allow + log	Although a printer can be a data leakage source, printing is a common user function within most organizations. This risk can be mitigated by physical and administrative controls.
PDA	Restrict, white list,	PDAs, mobile phones, imaging devices (such as

Setting	FISMA Setting	Rationale
Mobile Phones	log	scanners) and audio/video devices (such as MP3 players) present a clear risk to the control and protection of confidential data. The use of such devices should be blocked. Where required, the use of allowed devices is approved by device whitelist groups. Whitelists can be created based on vendor ID, product ID, or device serial number.
Imaging		
Audio/ video Devices		
Network Adapters	Allow	Network adapters allow the computer to be connected to a network. This is a common configuration and should not be blocked or logged.
Smart Cards	Allow	Smart Cards are commonly used as authentication devices. They do not pose a reasonable threat to network security.
Content security devices	Allow	Content security devices monitor the content of the flow of data to and from the endpoint. If such devices are present, they are usually part of a solution to enforce security and should not be blocked at the endpoint.
Un-classified devices	Block + Log	Unclassified devices are any devices that are not otherwise specified. These should not turn up very often, and present a clear risk to the confidential data.
Storage Control:		

Setting	FISMA Setting	Rationale
Autorun function	Block	A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat frequently used by malware and should be disabled by default.
Removable storage	Encrypt + log Apply File Control on files written to storage devices Apply File Control on Files Read from storage devices block smart functionality	Storage devices (such as USB drives) present a clear risk to confidential data. The organization should limit the use of storage devices to approved devices with the ability to appropriately encrypt the data. Use of these devices should be logged. A convenience feature of many operating systems is the ability to automatically execute a program upon the insertion of removable media. This feature, known as autorun or smart functionality, is also a security threat and should be disabled by default.
External HD	Encrypt + log	
CD/DVD	Encrypt + log Apply File Control on files written to storage devices Apply File Control on Files Read from storage devices Block unsupported burning formats	Certain formats for writing files to media such as CD or DVD do not support file logging. To preserve the logging settings for all files the "block unsupported burning formats" option should remain checked.
Floppy Drives	Read only + log	Because reading data from floppy disks is sometimes still required, the system allows read-only capability for such media.
Tape Drives	Block + log	As most users rarely use tape drives in their daily work, if at all, this option is blocked by default.
File Control	Log – write only	In order to support audit and investigation of security incidents involving confidential data, the organization should log all files written to external storage devices.
WiFi Network	Restrict, white list WPA encrypted networks, log	Wireless networks present a clear risk to the control and protection of confidential data. At the minimum, an organization should log any such behavior. Any use of Wi-Fi networks should be logged and limited to an approved list of Wi-Fi networks with proper encryption.
P2P	Block + log	
Policy Settings		

Setting	FISMA Setting	Rationale
Logging	Send logs to SafeGuard PortProtector Server Send logs every 12 hours Log connect and disconnect events	Logs should clearly not be stored on the endpoint, but instead sent to the SafeGuard PortProtector Server where they can be protected and viewed by the administrator. Other logging settings here provide adequate protection by ensuring periodic updating of logs on the server without burdening the network; inclusion of connect and disconnect events to allow for analysis of how long a device was connected.
End-user messages	Review the end user messages associated with the FISMA settings to ensure that they are consistent with your formally documented security policies and security awareness training program.	It is important to provide a constant reminder to personnel exposed to confidential data that they are responsible for protecting data and complying with policies. Modifying the end-user messages to specifically mention FISMA security and will assist in the security awareness of your organization.
Media Encryption	Do not allow users to access encrypted devices on computers outside of the network. Approve read only access for non-encrypted devices.	Using encrypted storage devices outside of the organization (at home or on external networks) poses a security threat of data leakage through unsecured networks. Setting read-only for non-encrypted devices allows the flexibility of importing information from removable storage devices without exposing confidential data to the risk of disclosure from loss or theft of a non-encrypted device.

16.2.2 Other SafeGuard PortProtector FISMA Settings

For the appropriate setting of other SafeGuard PortProtector features and options refer to the Pre-Requisites for Addressing FISMA Compliance Issues detailed in this document. Specifically, the following SafeGuard PortProtector features should follow the business objectives and the sensitive data environment, as defined in Foundations, Considerations, Preparations.

Logging of System Events

SafeGuard PortProtector alerts provide supervision of administrative actions and protection of the SafeGuard PortProtector security functions in case of attempted tampering. The following alert options should be set in order to preserve the security functions provided by SafeGuard PortProtector:

- Log all administrative events, logs all administrative actions and provides supervision of SafeGuard PortProtector administration.
- Alert all tampering events, detects tampering attempts and ensures the integrity of endpoint protection controls.

SafeGuard PortProtector Administration

SafeGuard PortProtector can be run by a single administrator or an organization may implement additional access control by defining additional administrators to a subset of administrative functions. This is an implementation of role-based access control and should be considered based on the organizations approach as defined in "Preparation 3: Determine Administrative Roles" which can be found under Preparations. Among the roles within the sensitive data environment the organization should consider are the following:

- Log Reviewer - Access to all logs and log functions, without the ability to edit policies.
- Policy Administrator - Access to edit and administer policies, without the ability to view logs.
- Audit - Read-only access to the administrators console, without the ability to perform any changes.

The setting of these roles should be based on the administration model and approach of the organization and the support needed for incident response and maintenance. Refer to Pre-Requisites for Addressing FISMA Compliance Issues for more complete instructions about SafeGuard PortProtector implementation preparation.

Domain Partitioning

Further access control granularity may be added with the SafeGuard PortProtector domain partitioning feature. The role-based access mechanism includes domain partitioning, which allows an administrator's role to be limited to a specific group of clients. This feature is useful in establishing the boundaries of the sensitive data environment by restricting the administrator's access within defined domains. The setting of these roles should be based on the organization's administration model and approach and the support needed for incident response and maintenance. Refer to Pre-Requisites for Addressing FISMA Compliance Issues for more complete instructions about SafeGuard PortProtector implementation preparation.

Administrative Password Strength

All passwords that protect system components within the sensitive data environment must comply with the organization's formally documented password policies. SafeGuard PortProtector Administrative Password strength rules apply passwords of all SafeGuard PortProtector administrators to the SafeGuard PortProtector Management Console, uninstall passwords of endpoint clients, and user passwords on encrypted devices.

Formally documented security policies are discussed in more detail in "Consideration 1: Policies and Procedures" in the Considerations section. Based on the organization's password strength policy, SafeGuard PortProtector administrative password strength criteria should be defined in the SafeGuard PortProtector to enforce organizational policies. Elements of the password strength include minimum length and required character types.

16.2.3 FISMA/SafeGuard PortProtector Feature Mapping

The following table provides a list of relevant FISMA requirements, and maps the relevant corresponding SafeGuard PortProtector features, and brief instructions on how to apply them. The full FISMA requirements list (updated to August 2009) can be found at the following link: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

Requirement Number	Requirement Description	Relevant SafeGuard PortProtector Features	How to apply SafeGuard PortProtector policies for FISMA compliance
AC-3 (1)	Access Enforcement: The information system restricts access to privileged functions and security-relevant information to explicitly authorized personnel.	SafeGuard PortProtector prevents the use of unauthorized devices on network computers, and can prevent certain file types from being copied to storage media. Different policies can be applied to different users, so authorized personnel can get higher permissions.	In the Policies World, create a New Policy, and configure it as needed. To set file type control, click the File Control tab in security policies.

Requirement Number	Requirement Description	Relevant SafeGuard PortProtector Features	How to apply SafeGuard PortProtector policies for FISMA compliance
AC-18 (1) (2)	Wireless Access Restrictions: The organization uses authentication and encryption to protect wireless access and scans for unauthorized wireless access points.	SafeGuard PortProtector allows the organization to create policies that force the use of encrypted Wi-Fi channels for secure transfer of data. These policies can even be set to require a specific level of encryption (e.g., WPA). In addition, SafeGuard PortProtector provides anti-bridging capabilities, preventing computers from connecting to wireless networks while connected to the organizational LAN.	Under port control, restrict Wi-Fi networks. Under Wi-Fi networks set a white list of approved Wi-Fi networks to WPA encrypted networks. To restrict anti-bridging, set "Hybrid Network Bridging" to Block.
AC-19	Access Control for Portable and Mobile Devices: The organization establishes usage restrictions and implementation guidance for portable and mobile devices; and authorizes, monitors, and controls device access to organizational information systems.	SafeGuard PortProtector provides the ability to control access to portable storage devices such as USB drives, PDAs, and mobile phones. The flexibility of SafeGuard PortProtector policies allows for a granularity of control that matchs the organization's needs. SafeGuard PortProtector also provides encryption	Configure SafeGuard PortProtector to control media and storage device use on desktops and laptops. The built-in FISMA policy provides explanations for these settings.

Requirement Number	Requirement Description	Relevant SafeGuard PortProtector Features	How to apply SafeGuard PortProtector policies for FISMA compliance
		for hard-disks and removable storage, so unauthorized users cannot access secure data.	
AC-20 (1)	Use of External Information Systems: The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in specific, authorized cases.	SafeGuard PortProtector contains the option of restricting the organization's encrypted storage device from being used outside of the organization. Using File Type Control, organizations can restrict the type of files that can be copied to/from external storage devices.	In security policies, under Media Encryption, make sure the "allow users to access devices on unprotected machines" option is not selected. To set File Type Control, click the File Control tab in security policies and choose which files should be restricted.
AU-2 (1) (2) (3)	Auditable Events: The information system provides the capability to compile audit records from multiple components throughout the system, manage selection, and update them as needed.	Sophos products provide extensive and granular logging options, collected in several log types: Client Logs File Logs Server Logs	Configure SafeGuard PortProtector to collect logs and send alerts according to your organization's policy. The built-in FISMA policy provides recommended pre-configured logging levels.
AU-3 (1) (2)	Content of Auditable Events: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the	SafeGuard PortProtector provides in-depth and granular logging and alerting options, both for security and administrative	For each action, set the Log and/or Alerts checkboxes for desired security actions.

Requirement Number	Requirement Description	Relevant SafeGuard PortProtector Features	How to apply SafeGuard PortProtector policies for FISMA compliance
	outcomes of the events, and to expand and centrally manage events throughout the system.	events.	
AU-6 (1) (2)	Audit Monitoring, Analysis, and Reporting: The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting, and employs automated mechanisms to alert security personnel of inappropriate or unusual activities.	SafeGuard PortProtector provides alerts, which can be sent immediately and automatically to outside sources such as mail, event viewer, or SNMP.In addition to SafeGuard PortProtector built-in alerting and reporting options, SafeGuard PortProtector also provides integration with SIEM systems, ensuring that security administrators can keep track of security events regardless of their chosen system.	In the Administration dialog, configure Alert Destinations. In security policies, under Alerts, choose the desired Destinations.
AU-8 (1)	Time Stamps: The information system provides time stamps for use in audit record generation, and allows synchronization with internal information system clocks.	SafeGuard PortProtector logs contain the time stamp of both the endpoint where the event originated from, as well as that of the management server.	To synchronize the time stamps, set both the server machine and endpoint machines to sync with network time servers. These settings are usually configured by default by the directory services.

Requirement Number	Requirement Description	Relevant SafeGuard PortProtector Features	How to apply SafeGuard PortProtector policies for FISMA compliance
CM-2 (1) (2)	Baseline Configuration: The organization develops, documents, and maintains a current baseline configuration and employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	SafeGuard PortProtector security policies contain extensive and granular definitions for restricting the use of ports, storage and non-storage devices, and enforcing restrictions. SafeGuard PortProtector includes a built-in policy server, which securely updates endpoint policies (either immediately from the server, or at periodic intervals). The server manages and displays the protection status, details, and log information of each endpoint. For CM-5, add info about role-based management and partitioning	In the Clients World, display network computers (search by name or by browsing directory tree), and view status and details of each computer. In security policies, configure automatic log retrieval and policy update interval either globally or per each policy separately.
CM-5 (1)	Access Restrictions for Change: The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.		
CM-6 (1)	Configuration Settings: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.		

Requirement Number	Requirement Description	Relevant SafeGuard PortProtector Features	How to apply SafeGuard PortProtector policies for FISMA compliance
CM-7 (1)	Least Functionality: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the functions and ports.	SafeGuard PortProtector security policies can be set to completely lock down organizational endpoint and allow only necessary permissions to approved users. Logs can be set to detect any unauthorized usage attempt. See also item MP-2.	In security policies, define which devices are allowed and blocked, or use the built-in FISMA policy with recommended, pre-configured permissions. Policies can be configured either for users or for computers, providing a high level of granularity of configuration.
CM-8 (1) (2)	Information System Component Inventory: The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	SafeGuard PortProtector maintains and displays a list of all computers in the organization and their current protection status. By using SafeGuard PortAuditor, it is possible to view all devices being used or previously connected to the network computers.	Open the Clients World to view network computers and filter them by status. Use SafeGuard PortAuditor to view all devices currently and previously connected to network computers.
CP-7 (1) (2) (3) (4)	Alternate Processing Site: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions.	SafeGuard PortProtector Management Server includes cluster support, for full redundancy and load-balancing.	When installing additional management servers, choose the "Cluster" installation option.

Requirement Number	Requirement Description	Relevant SafeGuard PortProtector Features	How to apply SafeGuard PortProtector policies for FISMA compliance
CP-9 (1) (2) (3) (4)	Information System Backup: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system.	SafeGuard PortProtector provides measures for creating encrypted backups of both the system configuration, and the security logs database.	In the Administration window, select *Maintenance* and choose backup options and schedule.
CP-10 (1)	Information System Recovery and Reconstitution: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.	SafeGuard PortProtectors provides an easy mechanism for recovering servers using backup keys.	In the SafeGuard PortProtector Install Wizard, choose the *Restore* option to import pre-existing backup keys and configuration.
IA-3	Device Identification and Authentication: The information system identifies and authenticates specific devices before establishing a connection.	SafeGuard PortProtector security policies can restrict access to storage and non-storage devices, and create exemptions based on vendor and product ID (for models), or serial number for specific devices, and log all access attempts according to VID, PID, serial number, user, and machine.	Set the security action for the device type to *restrict*, and select *white list* to add exemptions by VID, PID, or serial number.
IR-4 (1)	Incident Handling: The organization employs automated mechanisms to support the incident handling process.	By using alerts, it is possible to automatically receive real-time incident information notification.	Open the Administration dialog, click *Logs & Alert*s, and create new alert destinations. Set security policies to export alerts to
IR-5 (1)	Incident Monitoring: The organization employs automated mechanisms to		

Requirement Number	Requirement Description	Relevant SafeGuard PortProtector Features	How to apply SafeGuard PortProtector policies for FISMA compliance
	assist in the tracking of security incidents and in the collection and analysis of incident information.	Alerts can be exported to email, event viewer, syslog, and external systems, via SNMP or executable scripts.	them.
IR-6 (1)	Incident Reporting: The organization employs automated mechanisms to assist in the reporting of security incidents.		
MA-5	Maintenance Personnel: The organization allows only authorized personnel to perform maintenance on the information system.	SafeGuard PortProtector enables role-based management and domain partitioning. It is possible to define different administrative permissions for different system functions and only for specific parts of the network.	Open the Administration window. In General, under *Users Management* click the *Role Based (Advanced)* option, and define roles and domain partitions as needed.
MP-2 (1)	Media Access: The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.	SafeGuard PortProtector security policies provide granular policies to set in-depth permissions for device access and allow only necessary permissions. Logs can be set to detect any unauthorized usage attempt.	In security policies, define which devices are allowed and blocked, or use the built-in FISMA policy with recommended, pre-configured permissions.

Requirement Number	Requirement Description	Relevant SafeGuard PortProtector Features	How to apply SafeGuard PortProtector policies for FISMA compliance
MP-5 (1) (2)	Media Transport: The organization protects digital and non-digital media during transport outside of controlled areas and documents, where appropriate, activities associated with the transport of the media.	SafeGuard PortProtector provides built-in media encryption capabilities based on AES 256-bit encryption. Permissions can be set to limit use of encrypted devices to organizational computers only, or allow use outside of the network (offline) with password.	In security policies, under *Storage Control*, define which devices should be encrypted, or use the built-in FISMA policy with recommended, pre-configured settings, which by default encrypts all storage devices.
SI-4 (2) (4) (5)	Information System Monitoring Tools and Techniques: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.	SafeGuard PortProtector includes extensive logging, alerting, and shadowing capabilities, which notify administrators of any security incidents and the content of data copied to removable storage devices.	To set logging and alert levels for administrative events, open the Administration window and select *Logs & Alerts*. To set logging for security incidents, modify both security policies and *Global Policy Settings* as needed.
SI-5 (1)	Security Alerts and Advisories: The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.	SafeGuard PortProtector security policies include a large number of customizable end-user messages, which alerts the user of administrative changes (such as policy update), or security incidents (such as a device being blocked). Administrators can	In security policies, click the *End User Messages* tab, and modify end-user messages as needed.

Requirement Number	Requirement Description	Relevant SafeGuard PortProtector Features	How to apply SafeGuard PortProtector policies for FISMA compliance
		modify messages according to their needs.	
SI-7 (1) (2)	Software and Information Integrity: The information system detects and protects against unauthorized changes to software and information and employs automated tools that provide notification to appropriate individuals upon discovering discrepancies.	SafeGuard PortProtector includes redundant, multi-tiered anti-tampering measures, which prevent users from circumventing security policy. When such attempts are detected, the machine is automatically locked down, and logs and alerts are generated to notify security administrators.	SafeGuard PortProtector anti-tampering measures are enabled by default, and no administrator action is required. In addition, SafeGuard PortProtector encrypts all system logs and configuration files, and system communications, so they cannot be read or modified by unauthorized users.